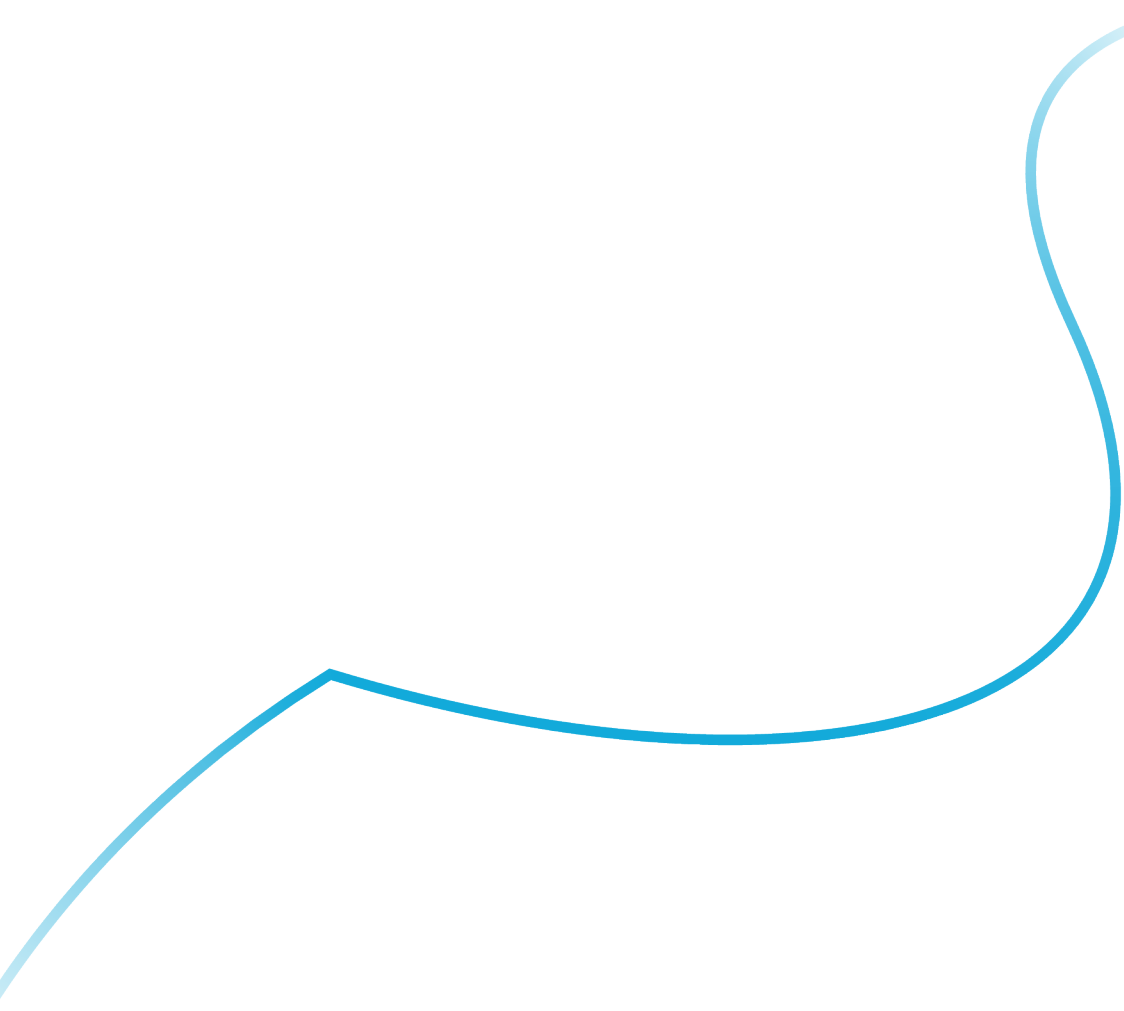
Trends in *Cybersecurity* 2024

Navigeren door de Cyberwereld

Capgemini



Trends in *Cybersecurity* 2024

Navigeren door de Cyberwereld

Inhoudsopgave

Interview:
Jerome Desbonnet - CTO and portfolio lead Capgemini
Navigeren door het complexe landschap van Cybersecurity
04

01 *Cyber Cluedo*: **Waarom staten besluiten hun cyberaanvallers publiekelijk te identificeren (of niet)**
Welke afwegingen zijn voor staten belangrijk wanneer zij ervoor kiezen om hun (cyber)aanvaller publiekelijk aan te wijzen?
Joanna van Let
06

02 **Cyberrisico's in de evoluerende** *OT-technologie*
Wat zijn de uitdagingen voor cyberweerbaarheid in 2024 binnen de OT-omgevingen?
Martijn Grootenboer, Rafik Nasari & Cathy Ellis
11

03 *Generatieve AI*: **het mes snijdt aan twee kanten voor cybersecurity**
Wat zijn de voordelen, risico's en bedreigingen van generatieve AI voor de cyberbeveiliging van een organisatie?
Ruben Tienhooven & Jean de Smidt
21

04 **De potentie ontgrendelen van** *AI in SAP-toegangsbeheer*

Op welke manier kan AI de beveiliging en efficiëntie van SAP Access Governance verbeteren?

Yunus Ceyhan, Ankit Arya & Kriti Biswas 26

05 *Versterk je weerbaarheid*: **de rol van GenAI bij de garantie van compliance**

Kan GenAI de weerbaarheid versterken en daarnaast voldoen aan de compliance eisen?

Rahul Rauniyar & Vera Irmak 32

06 **De Toekomst van** *Digitale Identiteit* **in Europa**

Is de EUDI Wallet een zegen of een bedreiging voor de samenleving?

Peter Hoogendoorn & Roy van der Koogh 40

07 *SecDevOps-processen* **implementeren terwijl teams het niet willen**

Hoe kan agile-ontwikkeling bijdragen aan consistentie en ervoor zorgen dat teams aan dezelfde beveiligingseisen voldoen?

Alex de Vries 49

Publicaties 55

Interview: Jerome Desbonnet

CTO en portfolio lead Capgemini

Jerome Desbonnet
CTO and portfolio lead Capgemini

Navigeren door het *complexe landschap* van Cybersecurity

Welkom bij de vierde editie van het Trends in Cybersecurity rapport.. Dit voorwoord is gebaseerd op een interview met onze CTO. In dit rapport navigeren we door de vele onderwerpen van cybersecurity en willen we het belang hiervan aanduiden in het huidige digitale landschap. Het thema is dan ook de navigatie door het complexe landschap van Cybersecurity. Digitale transformatie is overal en cyber en de beveiliging van cyber spelen een cruciale rol. We hopen u te kunnen begeleiden door de ontwikkelingen van de bits, de bytes en het altijd evoluerende landschap van cyber.

Het turbulente landschap

Het huidige landschap van cybersecurity wordt beïnvloed door gespannen geopolitieke situaties, uitdagingen rondom verkiezingsintegriteit, de impact van klimaatverandering en AI-gedreven technologieën, zoals de drastische verbetering van phishingmethoden, stemgebruik en deepfakes. Deze factoren creëren gezamenlijk een dynamische en uitdagende omgeving voor beveiligingsprofessionals. Recentelijk probeerde een team van hackers de stem van Jay Chaudhry, de CEO van Zscaler, te deepfaken om zijn werknemers geld over te laten maken. De poging mislukte. Er zijn echter ook voorbeelden van situaties die minder goed zijn afgelopen. In februari 2024 werd een financiële medewerker van een multinationaal bedrijf opgelicht en betaalde 25 miljoen dollar aan fraudeurs die deepfake-technologie gebruikten om zich tijdens een conference call voor te doen als de CFO van het bedrijf. Aangezien we grote bedrijven en overheden helpen hun systemen veilig te houden, moeten we constant waakzaam blijven voor deze ontwikkelingen, zoals de snelle evolutie van GenAI en de nieuwe wetten die ontwikkeld worden om hier vat op krijgen.

Nieuwe wetten omtrent AI

Nieuwe wetten en regelgeving, vooral met betrekking tot AI, worden op grote schaal ontwikkeld, met name in Europa. Deze nieuwe regelgeving vereist een grondige analyse van modellen om te waarborgen dat AI-systemen veilig en compliant zijn. Dit nieuwe landschap brengt aanzienlijke uitdagingen met zich mee, maar ook kansen voor cybersecurity en vraagt om een diepgaande beoordeling van AI-modellen.

GenAI brengt nog een uitdaging met zich mee: namelijk om bedrijfsactiva te beschermen wanneer gebruikers data genereren. Het is bijvoorbeeld belangrijk om te voorkomen dat werknemers per ongeluk vertrouwelijke gegevens delen via AI-tools zoals Copilot of ChatGPT. Gegevens die met deze tools worden gedeeld, worden, in de meeste situaties, eigendom van ChatGPT, wat mogelijk gevoelige informatie blootstelt. We moeten ons altijd bewust zijn van de implicaties van het gebruik van AI-tools en ervoor zorgen dat er beveiligingsmaatregelen zijn om datalekken en ongeautoriseerde toegang te voorkomen. Dit houdt ook het opleiden van werknemers over de risico's van door AI gegenereerde gegevens in en het implementeren van een goed beveiligingsbeleid om deze nieuwe uitdagingen aan te pakken.

GenAI: transformatie van zowel (cyber)aanval als verdediging

Een van de grootste en snelste ontwikkelingen is de vooruitgang van GenAI. GenAI transformeert zowel aanvallende als verdedigingsmechanismen in cybersecurity. Cybercriminelen gebruiken de tool om efficiëntere phishing-methoden en deepfakes te creëren, terwijl verdedigers GenAI-tools zoals Microsoft's Copilot inzetten voor een betere beveiliging. Deze

technologieën brengen echter nieuwe uitdagingen met zich mee, zoals het risico op misbruik van door AI gegenereerde data en het waarborgen van de veiligheid van bedrijfsactiva.

Het gebruik van GenAI kan worden gecategoriseerd op vier manieren:

1. **GenAI aangedreven kwaadwillende activiteiten:** Het creëren van geautomatiseerde aanvallen, phishing-methoden en deepfakes. Aanvallers kunnen GenAI gebruiken om zeer overtuigende phishing-emails en realistische deepfakes te maken, waardoor het gemakkelijker wordt om slachtoffers te misleiden en traditionele beveiligingsmaatregelen te omzeilen.
2. **Beter en sneller beveiligingsbeslissingen nemen met GenAI:** Het gebruik van tools zoals Copilot voor beveiligingsverbetering. Verdedigende partijen kunnen GenAI gebruiken om hun verdediging te versterken, dreigingsdetectie en -respons te automatiseren en de algehele beveiligingshouding te verbeteren. Producten van bedrijven zoals Microsoft, Google en Vectra zijn voorbeelden van deze defensieve toepassing van GenAI.
3. **Bescherming van bedrijfsactiva en reputatie met behulp van GenAI:** Aanpakken van aanvallen op generieke AI-systemen. Naarmate aanvallers zich richten op het uitbuiten van kwetsbaarheden in AI-systemen, wordt het essentieel om deze systemen te beschermen tegen compromitterende input. Dit behelst onder andere het beveiligen van AI-modellen tegen vijandige aanvallen die hun output kunnen manipuleren en zo uw intellectuele eigendom kunnen aanvallen of persoonlijke gegevens binnen AI-systemen die medewerkers mogelijk gebruiken.
4. **GenAI-oplossingen bouwen met ethiek en veiligheid als kern:** Dit houdt in dat u op dreigingen anticipeert en het gebruik vermijdt van AI-systemen die opzettelijk voor kwaadwillige activiteiten zijn gecreëerd. AI-systemen om te vermijden betreffen systemen met een gebrek aan ethiek, maar ook een gebrek aan bias, of andere ongewenste resultaten. Deze vorm van bescherming heeft betrekking op het kiezen van ethische partners in plaats van goedkopere en het evalueren en beschermen van de kwaliteit van trainingsdata. Het is essentieel om ervoor te zorgen dat bedrijfsgegevens en activa niet worden blootgesteld of geëxploiteerd door dergelijke systemen.

Een opkomende dreiging: kwantumcomputing

Kwantumcomputing staat op het punt om een revolutie te veroorzaken binnen cybersecurity en vormt een grote bedreiging. Traditionele versleutelingsmethoden kunnen binnenkort verouderd raken omdat kwantumcomputers de tijd die nodig is om versleuteling te kraken drastisch verkorten. Overheden en organisaties moeten zich voorbereiden op een toekomst waarin kwantumcomputing kan worden gebruikt voor spionage en het kraken van beveiligingssystemen. Dit betekent ook het overwegen van lange termijn gegevensbeveiliging en het ontwikkelen van post-kwantum versleutelingsmethoden. Gegevens die vandaag de dag worden vastgelegd vanwege hun lange-termijnwaarde, zoals nucleaire strategieën of lange termijn patronen in gegevens, lopen gevaar. Dit vormt een bedreiging voor onze persoonlijke gegevens, zoals paspoorten, geboortedata en gegevens die nodig zijn voor hypotheken. Denk aan de sleutel om de gegevens in de NFC-chip in een paspoort te versleutelen. Die heeft een waarde van tien jaar. Kwantumcomputing ontwikkelt zich echter heel snel en de gloednieuwe paspoorten van vandaag zullen gekraakt zijn voordat ze verlopen.

Wat zouden bedrijven moeten doen?

Laten we eerlijk zijn: perfectie in cybersecurity bestaat niet. De strijd tussen cyberaanvallen en cyberverdediging is een constante race tussen snel ontwikkelende technologieën. Om onze bedrijven veilig te maken, moeten we iedereen leren zichzelf zo goed mogelijk te verdedigen en hun medewerkers bewust te maken van de uitdagingen. Succesvolle cyberaanvallen zullen uiteindelijk iedereen treffen. U moet klaar zijn wanneer het gebeurt. Detecteer de aanval snel en beperk de impact. Train uw medewerkers om continu verificatievragen te stellen en herhaal noodscenario's regelmatig. Veilig blijven in een digitale wereld is essentieel. Maar onthoud dat het nog steeds mensen zijn die de systemen controleren.

In dit rapport navigeren we door verschillende cybersecurityonderwerpen zoals AI, privacy en digitale identiteit. We hopen dat u geniet van deze vierde editie van Trends in Cybersecurity en dat het u inzicht biedt in de uitdagingen en kansen voor een veilige toekomst.

01

Cyber Cluedo: Waarom staten besluiten hun cyberaanvallers publiekelijk te identificeren (of niet)

Welke afwegingen zijn voor staten belangrijk wanneer zij ervoor kiezen om hun (cyber)aanvaller publiekelijk aan te wijzen?

Highlights

- Cyberaanvallen zijn relatief goedkoop en kunnen worden uitbesteed aan individuen of hackersgroepen. Dit maakt het moeilijk om de juiste aanvallende partij aan te wijzen en om de schuld en gevolgen van dergelijke aanvallen bij de juiste agressor te leggen.
- Bij zowel politiek als nationale veiligheid is informatie cruciaal. Het verkrijgen van informatie is belangrijk, maar hoe je hier vervolgens op reageert misschien nog wel meer. Bepalen welke kaarten je laat zien en welke je verborgen moet houden, vereist een voortdurende kosten-batenanalyse.
- Waarschijnlijk zullen staten hun digitale aanvaller steeds vaker via diplomatieke kanalen te confronteren zijn plaats van publieke beschuldigingen te uiten.
- Voor velen van ons lijkt 'attributie' een natuurlijke reactie op een onrecht. Onrecht moet immers worden uitgesproken en de verantwoordelijke partij moet ter verantwoording worden geroepen. Maar wanneer het gaat om militaire, veiligheids- of strategische (staats)belangen, moet de beslising om publiekelijke beschuldigingen te uiten zorgvuldig worden overwogen.

De term 'attributie' betekent in essentie het openbaren van een aanvallende actor zoals een land, organisatie of individu, door hen publiekelijk verantwoordelijk te houden voor een aanval. Dit betekent niet dat de dader ook direct ter verantwoording wordt geroepen, maar wel dat zij door het slachtoffer publiekelijk worden aangeduid als de veroorzaker van de aanval. Attributie kan worden vergeleken met het spel Cluedo. De vraag rijst wat staten ertoe brengt om op het internationale toneel te zeggen: "Ik denk dat het land X was, dat met een zero-day-exploit mijn kritieke infrastructuur heeft aangevallen."

Attributie in de publieke sector

Cyberaanvallen en cybercriminaliteit gerelateerd aan overheidsinstellingen of staatsfuncties moeten fundamenteel anders worden bekeken dan aanvallen op bedrijven. Voor bedrijven is de vraag 'wie heeft het gedaan', de whodunit, minder belangrijk omdat (als we het plat slaan) een aanval alleen de winstmarge beïnvloedt. Dat is natuurlijk geen kleinigheid, maar voor overheden is de 'wie' net zo belangrijk als de 'hoe' of 'waarom'. Het ontdekken van de identiteit van de dader bepaalt namelijk de manier waarop overheden omgaan met de aanval en wat ze kunnen leren over de aanvallende partij.

Een bedrijf zal minder geïnteresseerd zijn wie er precies achter een cyberaanval zit, zo kan het bedrijf A, B of C zijn. Maar een overheid moet op basis van strategische belangen weten waar de dreiging vandaan komt. Het zou bijvoorbeeld heel onverstandig zijn om een bondgenootschap aan te gaan met een land waarvan je weet dat dit land je probeert aan te vallen. Neem bijvoorbeeld de vele dijken die Nederland beschermen tegen het zeewater, de besturingssystemen die zorgen voor schoon water, de luchtverkeersleidingsinformatie voor zowel commercieel als militair gebruik, of systemen die in de gaten houden welke entiteiten er op dit moment aanwezig zijn in het Nederlandse luchtruim. Het is belangrijk om erachter te komen wie hierin een interesse toont, bijvoorbeeld als het gaat om spionage of het verstoren van functionaliteiten, zoals de dijken. Als het gaat om de continuïteit van een bedrijf, is weten wie er achter de aanval zit minder belangrijk dan weten wat de bedrijfsvoering verstoort. Voor regeringen en het functioneren van staten is de 'wie' echter net zo belangrijk.

Een bedrijf zal minder geïnteresseerd zijn wie er precies achter een cyberaanval zit, zo kan het bedrijf A, B of C zijn. Maar een overheid moet op basis van strategische belangen weten waar de dreiging vandaan komt.

Cyberaanvallen en spionage

Het zal voor niemand als verrassing komen dat cyberaanvallen toenemen. Oorzaak is dat ze relatief goedkoop zijn, veiliger zijn dan traditionele oorlogsvoering en niet van doen hebben met het gros van de moeilijkheden en beperkingen van traditionele oorlogsvoering. Bovendien is het veel gemakkelijker om cyberaanvallen uit te besteden door bijvoorbeeld een groep hackers samen te stellen en deze te sponsoren. Cyberaanvallen zijn geen nieuw fenomeen, maar zijn de afgelopen twee jaar wel aanzienlijk toegenomen, vooral vlak voor de Europese verkiezingen van mei 2024. Duitsland, Polen en Tsjechië hebben alle drie aanvallen gemeld van een staatsgecontroleerde hackergroep genaamd Fancy Bear (ATP28).[1] Ook Nederland werd slachtoffer van een aanval die naar alle waarschijnlijkheid verband hield met de Europese verkiezingen. De dag voor de verkiezingsdag hebben Cloudflare-systemen een DDoS-aanval gedetecteerd en gemitigeerd die op minstens twee websites van Nederlandse politieke partijen waren gericht.[2] Eerder dit jaar riep Nederland voor het eerst publiekelijk een andere staat ter verantwoording vanwege het hacken van het Nederlandse defensienetwerk. De Nederlandse minister van Defensie stelde dat het publiekelijk benoemen van de dader zou zorgen voor 'het vergroten van de internationale weerbaarheid tegen dit soort cyberspionage'.[3]

Wat maakt attributie een aantrekkelijke aanpak?

Staten kunnen om verschillende redenen aan cyber attributie doen. Ze kunnen anderen oproepen om normatieve redenen, oftewel: om 'de norm vast te stellen'. Deze aanpak wordt vaak gebruikt door westerse landen, waaronder Nederland. Het openlijk ter verantwoording roepen op het internationale toneel is belangrijk, aangezien staten als Nederland floreren bij een vredig internationaal speelveld waar internationaal recht en de handhavende instituties worden geëerd. Door gebruik te maken van deze instituties en internationaal recht dwingen westerse mogendheden een bepaalde norm af. Deze benadering kan op verschillende geïnterpreteerd worden: men probeert een mondiale 'heerschappij' af te dwingen waarbij het aanvallen van elkaars functionaliteiten, instellingen en de democratie niet wordt getolereerd en openlijk wordt veroordeeld. Binnen de politieke wetenschappen wordt dit 'naming-and-shaming' genoemd. Door vast te stellen dat een handeling verkeerd is, creëert deze benadering ook een norm voor wat wél goed is. Echter, deze aanpak werkt alleen als je te maken hebt met een dader die waarde hecht aan algemeen goedgekeurde normen en waarden.

Afschrikking gaat hand in hand met het concept naming-and-shaming. Staten kunnen attributie gebruiken om de agressor af te schrikken. Deze benadering is gebaseerd op twee

[1] https://www.politico.eu/article/poland-targeted-russia-hackers-germany-czechia-malicious-cyber-campaign/
[2] https://blog.cloudflare.com/dutch-political-websites-hit-by-cyber-attacks-as-eu-voting-starts
[3] MIVD onthult werkwijze Chinese spionage in Nederland | Nieuwsbericht | Defensie.nl

De eerste stap van attributie vindt plaats nadat je hebt gemerkt dat je bent aangevallen of dat je systemen zijn gecompromitteerd.

belangrijke uitgangspunten. Ten eerste, dat de dader wordt afgeschrikt door het idee om publiekelijk benoemd te worden wat deze ervan weerhoudt soortgelijke technieken te gebruiken om opnieuw aan te vallen. Ten tweede, door een agressor te benoemen, laat je ook zien dat je over de vaardigheden en kennis beschikt om zijn aanval te detecteren en/of te stoppen. Dit kan op twee manieren worden geïnterpreteerd: je kunt de agressor laten weten dat een toekomstige aanval zinloos is, maar je kunt ook je kaarten laten zien; Andere (staats)actoren weten dan over welke capaciteiten jouw veiligheidsdiensten beschikken.

Misschien verwacht je geen directe aanval. Maar stel dat er een scenario ontstaat waarbij een agressieve staat een tweeledige aanval uitvoert. Als een staatsfunctionaris vervolgens aankondigt dat er bewijs is van een aanval, kan dit betekenen dat slechts een deel van het bewijs onthuld kan worden of dat slechts één aspect ervan gedeeld wil worden. Het gebruik van attributie op deze manier kan toekomstige aanvallen afschrikken, tegelijkertijd (maar tegelijkertijd worden) wel de capaciteiten van de veiligheidsdiensten blootgegeven. Door het bewijsmateriaal over een aanval en de daarbij gebruikte methoden openbaar te maken, zorg je er waarschijnlijk wel voor dat de aanvallende TTP's (tactieken, technologieën en procedures) waardeloos worden, omdat andere staten nu weten waar ze op moeten letten.

Wat maakt attributie moeilijk?

De eerste stap van attributie vindt plaats nadat je hebt gemerkt dat je bent aangevallen of dat je systemen zijn gecompromitteerd. Je kunt geen aanval toeschrijven aan een ander als je niet zeker weet naar wie je kunt wijzen. Uitgebreid onderzoek en bewijs zijn dus nodig. Simpel gezegd, als je niet alle feiten hebt, is het misschien het beste om af te wachten of om je bondgenoten te vragen of zij vergelijkbare problemen hebben. Zo vertelden Nederlandse veiligheidsdiensten in 2018 over de nauwe samenwerking met de Amerikaanse en Britse veiligheidsdiensten.[4]

Staten kunnen er ook voor kiezen om bepaalde informatie niet openbaar te maken en in plaats daarvan de kennis van een aanval als een strategische (onderhandelings)troef te bewaren. In 2018 spraken de Nederlandse inlichtingendiensten over een verijdelde spionagepoging door een andere staat, waarbij enkele individuen

Afbeelding 1: *Voor- en nadelen van cyberattributie*

Voordelen van het publiekelijk attribueren van een aanval	Nadelen van het publiekelijk attribueren van een aanval
Normen stellen	Grondig bewijs / zekerheid vereist
Afweer van toekomstige aanvallen	Actoren kunnen onverschillig zijn
Vermindert de kans dat geïdentificeerde TTP's in de toekomst worden gebruikt.	Je kunt je kaarten op tafel leggen door openlijk over de aanval te spreken

[4] https://english.defensie.nl/topics/cyber-security/documents/publications/2018/10/04/remarks-minister-of-defense-4-october-in-the-hague
[5] https://english.defensie.nl/topics/cyber-security/documents/publications/2018/10/04/remarks-minister-of-defense-4-october-in-the-hague
[6] https://www.consilium.europa.eu/en/press/press-releases/2024/06/24/cyber-attacks-six-persons-added-to-eu-sanctions-list-for-malicious-cyber-activitiescyberattacks-against-eu-member-states-and-ukraine/
[7] Defensie Cyber Strategie 2018: Investeren in digitale slagkracht voor Nederland, Ministerie van Defensie, november 2018

toegang probeerden te krijgen tot informatie van de Organisatie voor het Verbod op Chemische Wapens (OPCW). De Nederlandse Staat maakte deze informatie openbaar op hetzelfde moment dat het Amerikaanse ministerie van Justitie de aanklacht openbaar maakte in een zaak tegen de cyberoperaties van een aanvallende staat.[5] Een andere strategische keuze om niet publiekelijk naar buiten te komen over een cyberaanval tegen jou, kan zijn wanneer je als staat betrokken bent bij soortgelijke activiteiten. Het is dan natuurlijk een groot risico om gezichtsverlies te lijden als je een staat beschuldigt van hetzelfde misdrijf dat je zelf pleegt.

Het hebben van de juiste informatie is belangrijk, maar weten naar wie deze informatie leidt is evenzo belangrijk. Staten kunnen kwaadaardige cyberactiviteiten uitbesteden aan hackers, waardoor ze de schuld gemakkelijk kunnen afschuiven, mits hun sporen goed zijn uitgewist en er voldoende afstand bestaat tussen de staat en de hackers of hackergroepen. Door de verantwoordelijkheid weg te nemen bij de staat zelf, hebben deze groepen in wezen een carte blanche om te opereren zoals ze willen. Wanneer getroffen landen op hun beurt deze actoren willen 'straffen' voor de cyberaanvallen, hebben staten weinig andere keuzes dan sancties op te leggen aan de opgespoorde individuen,[6] in plaats van het bewijsmateriaal terug te kunnen leiden naar statelijke actoren.

Gebeurt attributie daadwerkelijk?

Attributie gebeurt wel degelijk, en er zijn voorbeelden van staten die hebben verklaard dat attributie essentieel is voor hun veiligheidsbeleid, waaronder Nederland. In de Nederlandse cyberstrategie wordt attributie specifiek genoemd. Het Nederlandse kabinet is van mening dat "een actief politiek attributiebeleid bijdraagt aan de afschrikkende werking en Nederland een minder aantrekkelijk doelwit maakt voor cyberaanvallen".[7]

Maar wanneer we kritisch kijken, moeten we ons afvragen of een agressor die overweegt een ander land aan te vallen, of misschien malware plant voor toekomstige aanvallen of verstoringen, het iets uitmaakt om publiekelijk te schande te worden gemaakt. Uiteindelijk hangt de keuze met wie we een bondgenootschap willen sluiten, de beslissing welke informatie we met wie willen delen en de beslissing wanneer we met de vingers gaan wijzen, allemaal af van de politieke en strategische beslissingen die door regeringen worden genomen. Politici zullen moeten kijken naar de voor- en nadelen (zie afbeelding 1) van het openbaar maken van een aanval, en of het in het landsbelang is om de zaak in plaats daarvan stilletjes op te lossen.

We moeten ervan uitgaan dat staten hun aanvallers vaker achter gesloten deuren confronteren en proberen de aanval achter de hand te houden om deze op een later tijdstip te gebruiken of om deze kwesties via diplomatie op te lossen als wordt besloten dat dit de beste en veiligste werkwijze is. Uiteindelijk zal de stille en strategische diplomatieke route het vaak winnen van de wijzende vinger.

Nb. Dit artikel is op geen enkele wijze Gebaseerd op activiteiten of informatie van klanten. Dit onderzoek is onafhankelijk uitgevoerd.

Over de auteurs:

Joanna van Let

Voormalig Cybersecurity Strategy Consultant
Momenteel Engagement Manager

Joanna is afgestudeerd in politieke wetenschappen, met een focus op Europese politiek en internationale betrekkingen. Haar onderzoek richtte zich op het buitenlandse beleid van Nederland en cyberagressie door staten. Ze blijft geïnteresseerd in het snijvlak tussen (cyber)veiligheid en politiek.

www.linkedin.com/in/joannavanlet/
Joanna.van.a.let@capgemini.com

02

Cyberrisico's in de evoluerende *OT-technologie*

Wat zijn de uitdagingen voor cyberweerbaarheid in 2024 binnen de OT-omgevingen?

Highlights

- Dreigingen voor kritieke infrastructuur door statelijke actoren nemen toe door geopolitieke spanningen en de toenemende mate cyber criminaliteit.
- OT-omgevingen raken steeds meer vervlochten met IT-innovaties zoals (I)IoT en als gevolg daarvan ook met het internet.
- De bescherming van OT-omgevingen loopt nog altijd achter ten opzichte van IT-omgevingen.
- NIS2 verplicht bedrijven zich actiever in te spannen voor het beveiligen van hun en incidenten te melden.
- NIS2 biedt kansen om samen met overheidsinstanties zoals het NCSC-cyberdreigingen het hoofd te bieden.

De opkomst van OT-technologieën heeft de manier waarop industriële processen en systemen worden beheerd getransformeerd. Deze technologische vooruitgang brengt echter ook nieuwe cyberrisico's met zich mee, die toenemen naarmate OT- en IT-technologie verder consolideren. Dit zorgt voor een veranderend cyber krachtveld, beïnvloed door zowel de technologische veranderingen als geopolitieke spanningen en de sterke groei in cybercrime. Daarnaast worden nieuwe wetgevingen en richtlijnen steeds complexer.

Operationele omgevingen

Digitalisering van OT-omgevingen levert voordelen op. Het zorgt onder andere voor snelheid, efficiëntie, stroomlijnen van productieprocessen en ondersteunen van 'just-in-time' logistieke processen. Echter, is het toepassen van cyberweerbaarheid in OT-omgevingen achtergebleven. Voorbeelden uit de praktijk zijn langere lifecycle tijden, standaard wachtwoorden, onbeveiligde communicatie, geen of weinig patch management en onvoldoende dekking van antivirus applicaties. Redenen hiervoor zijn: gebrek aan kennis en kunde omtrent cybersecurity, gebrek aan awareness, bereidheid tot implementatie van cybersecuritymaatregelen en beperkt budget. Cybersecurity wordt vaak gezien als een kostenpost, terwijl het in werkelijkheid een middel is om de winst te beschermen en ervoor te zorgen dat organisaties door kunnen blijven gaan met hun operaties.

Toename van IIoT in de operationele omgeving

IoT (Internet of Things) is niet meer weg te denken uit onze huidige maatschappij. IoT zijn slimme apparaten die verbonden zijn op het netwerk. Voor OT biedt de introductie van IIoT (Industrial Internet of Things) kansen voor predictive maintenance, zoals kortere proces stoptijden en minder schade door acute defecten. Het maakt ook de analyse van OT-processen makkelijker, wat de efficiëntie kan vergroten.

Deze toename kent echter ook risico's. Het betekent een verdere convergentie met de IT-omgeving en verbinding met het internet om data te verzamelen en te analyseren. Daarnaast wordt OT-netwerk complexer waarbij het verkeerd aansluiten van componenten het aanvalsoppervlakte vergroot. IoT apparaten bieden ook kansen voor kwaadwillende om ongewenste toegang te verkrijgen tot het netwerk. Deze slimme apparaten zijn doorgaans ondermaats beveiligd, zoals door onveilige standaard instellingen, standaard wachtwoorden, onvoldoende databeveiliging en onveilige update mechanismes.[1]

Dreigingen binnen OT-landschap ligt op loer

Onderzoek laat zien dat cyberaanvallen op organisaties bij alle industrieën zijn toegenomen ten opzichte van dezelfde periode vorig jaar.[2] In 2023 waren de meeste aanvallen gericht op spionage, het verstoren van industriële processen en ransomware. Vaak zijn grote organisaties, die maatschappelijk belangrijk zijn, het doelwit. Daarnaast blijft spionage een zorgelijke ontwikkeling gezien de toenemende mate van protectionisme en de verontrustende geopolitieke situatie. Dit vraagt om een geïntegreerde aanpak van security, waarbij organisaties niet alleen de bekende grenzen van hun IT-omgeving beschermen, maar ook aandacht besteden aan de gevoeligheid van hun OT-omgeving, operationele processen, procedures en technologieën.

Deze aanpak leidt veelal tot groter bewustzijn over de kwetsbaarheid van OT-systemen binnen organisaties.

[1] https://claroty.com/blog/iiot-security-essentials
[2] https://www.fortinet.com/resources/reports/state-of-ot-cybersecurity

Verschillende westerse veiligheidsdiensten zien de volgende drie trends:[3]

1. Geopolitieke ontwikkeling

De geopolitieke situatie is de afgelopen jaren verhard, waardoor statelijke actoren vaker cyberaanvallen gebruiken om hun belangen te behartigen. Deze dreigingen kunnen ook het OT-landschap raken, zoals gezien in de oorlog in Oekraïne.[4] [5] OT-processen, vaak van nationaal belang, kunnen bij falen leiden tot maatschappelijke ontwrichting. Daarom is de focus op het standaardiseren en borgen van deze processen nog nooit zo groot geweest, vooral in sectoren als transport en nutsvoorzieningen. Een grote storing zou veel schade kunnen aanrichten met gevolgen voor mens en milieu. Statelijke actoren investeren fors in offensieve cybercapaciteit, waardoor ze een grotere bedreiging vormen voor organisaties. Aanvallen kunnen OT-processen verstoren of saboteren, en digitale spionage is ook een serieuze bedreiging die als businessrisico moet worden meegenomen.

2. Cybercrime

Georganiseerde criminelen voeren inmiddels ook specifieke aanvallen uit binnen het OT-landschap.[6] Ransomware aanvallen, waarbij systemen gegijzeld worden, blijven populair. Deze aanvallen worden vaak grensoverschrijdend uitgevoerd vanuit landen waar opsporing bijna onmogelijk is. Bij ransomware aanvallen worden organisaties gedwongen losgeld te betalen voor een ontgrendelingssleutel. Omdat OT-processen van groot belang zijn, wordt er door de organisatie grote sommen losgeld betaald.[7] Uit verschillende onderzoeken blijkt dat ieder jaar het record wordt gebroken van het aantal succesvolle ransomware aanvallen.

3. Interne dreigingen

Interne dreigingen, al dan niet opzettelijk, worden veroorzaakt door personen die een relatie hebben met de organisatie.[8] Spionage, actueel tijdens de Koude Oorlog, lijkt weer terug te zijn, ook in Nederland.[9] Naast opzettelijke acties vormen menselijke fouten ook een risico.[10] Interne dreigingen worden vaak over het hoofd gezien bij cyberdreigingen, omdat medewerkers vaak onbewust onveilig handelen. Van de organisaties die in 2023 ervaring hadden met een cyberaanval, gaf meer dan de helft (55%) aan dat phishing-e-mails de oorzaak waren.[11] Onvoldoende governance en onduidelijke verantwoordelijkheden bij OT-installaties leiden tot inherente kwetsbaarheden.

Afbeelding 1: *OT versus IT*

Operationele Technologie (OT)	Informatie Technology (IT)
Eerste prioriteit is veiligheid, tweede is beschikbaarheid, daarna integriteit en vertrouwelijkheid	Eerste prioriteit is vertrouwelijkheid
Installaties die vaak 10 en niet uitzonderlijk 30 jaar zonder revisie draaien	lifecycle management zorgt voor regelmatig vervanging van hardware
Processen die volledig afhankelijk zijn van verouderd, slecht gedocumenteerde	Software updates worden continu gepushed
Stakeholders minder vertrouwd met digitale onderhoud - wel met mechanische zoals lagers en olie	Overeenkomst met business stakeholders over maintenance windows bijvoorbeeld buiten kantooruren of buiten de jaar afsluiting
Gespecialiseerde installaties en apparatuur en ontwikkelomgeving om proef te draaien	Commodity platformen: test en ontwikkelstraten normaliter aanwezig
Industriële omgeving bevat apparatuur van vele bronnen; integrale testing van het end-to-end process vraagt om aanwezigheid van dure specialisten, gecoördineerde inzet en strakke planning	Aantal leveranciers beperkt, remote update mogelijk, terugdraaien
Remote locaties met laag capaciteit netwerkverbinding vermoeilijkt het betrouw oversturen van updatebestanden	Netwerkverbinding is geen beperkende factor
Installaties ontoegankelijk – bijvoorbeeld op zee, onderwater, en andere voor mensen onveilige omgevingen zoals kerncentrale, chemicaliën fabriek	Fysieke locatie is meestal bereikbaar en mens vriendelijk
Security bewust zijn onder OT-personeel is niet vanzelfsprekend	IT-personeel is goed op de hoogte van cyberdreigingen en praktijken

[3] https://www.ncsc.nl/binaries/ncsc/documenten/publicaties/2023/juli/3/cybersecuritybeeld-nederland-2023/CSBN+2023.pdf
[4] https://cyberscoop.com/frostygoop-ics-malware-dragos-ukraine/
[5] https://www.reuters.com/world/europe/icc-probes-cyberattacks-ukraine-possible-war-crimes-sources-2024-06-14/
[6] https://www.enisa.europa.eu/publications/enisa-transport-threat-landscape

Aanvallen op IT-systemen verplaatsen naar OT-systemen

Veel aanvallen op OT-systemen lijken zich te richten op oudere apparatuur met ongepatchte software, wat erop wijst dat OT-omgevingen steeds vaker het doelwit worden van op IT gebaseerde legacy aanvallen die niet langer effectief zijn tegen IT-systemen.[12] De industrie als geheel ziet echter ook een verontrustende toename van speciaal gebouwde OT aanvallen die gericht zijn tegen SCADA (Supervisory Control and Data Acquisition) en ICS (Industrial Control System).[13] Door de groter geworden koppeling tussen de IT- en OT-omgeving, kan een aanval op één van deze omgevingen direct invloed uitoefenen op de andere. Het is daarom ook belangrijk om preventieve controls, zoals netwerksegmentering en firewalls, en detectie controls, zoals SOC-diensten, in te richten binnen het OT-landschap.

OT-monitoring wordt steeds complexer en belangrijker

Voor een goed functionerende OT SOC (Security Operations Center) is het monitoren van het OT-landschap essentieel. Echter, het toepassen van monitoring blijft in het OT-landschap achter. Eén verklaring hiervoor is de gewoonte het OT-landschap niet remote toegankelijk te maken, van oudsher minder noodzaak voor was.

De behoefte om op afstand te werken in OT-omgevingen is mede ontstaan tijdens de Covid-19 periode toen het aantal medewerkers op locatie omlaag moest,[14] en door technologische ontwikkelingen zoals de introductie van cloud toepassingen en (I)IoT.[15] Belangrijk te vermelden is dat IT- en OT-monitoring geen ‘one-size-fits-all’ is. Protocollen die gebruikt worden binnen OT zijn specifiek voor een fabrikant. Monitoring tools voor OT zijn daarom ook vaak specifiek bedoeld voor ***die*** omgeving. Monitoring in OT heeft ook andere doeleinden. Zoals bijvoorbeeld het onderkennen van een ‘dual homed’ systeem, een systeem dat een directe verbinding heeft met twee levels in het Purdue model[16] waarmee firewalls omzeild kunnen worden.

Door de grote schaal en wijde spreiding van installaties, zoals bij slimme meters, boorplatformen en spoor wissels, is het detecteren van ongeoorloofde systemen van belang. Bijvoorbeeld onbekende 4G modems en draadloze toegangspunten die als achterdeur gebruikt kunnen worden[17].

Om de mix nog complexer te maken hebben we te maken met (I)IoT apparaten en technologieën zoals drones die een fysieke bedreiging

[7] https://ransomwhe.re/
[8] https://www.rtl.nl/rtl-nieuws/artikel/5360161/spionage-rusland-zweden-geheime-dienst-groe-sapo-oorlog
[9] https://nos.nl/artikel/2448320-dit-weten-we-over-de-russische-spionnen-in-nederland
[10] https://nos.nl/artikel/2511530-duitse-defensieminister-afluisteren-gesprek-kon-door-fout-officier
[11] https://www.channelconnect.nl/security-en-privacy/helft-organisaties-kreeg-in-2023-te-maken-met-data-aanvallen/
[12] https://www.darkreading.com/ics-ot-security/to-damage-ot-systems-hackers-tap-usbs-old-bugs-and-malware

of surveillance mogelijkheid bieden aan actoren. Deze surveillance kan via audio en video opnames, maar ook het analyseren van het draadloze netwerk. Ook deze nieuwe dreigingen moeten gedetecteerd worden.[18] [19] Het valt te verwachten dat dit op termijn ook verplicht gesteld gaat door overheden.

Het monitoren van het OT-netwerk maakt inzichtelijk welke systemen aanwezig zijn, zodat de asset management informatie bijgewerkt kan worden en het helpt om dreigingen te onderkennen en maatregelen te nemen. Afwijkingen in netwerkverkeer kunnen wijzen op actieve actoren. Het correleren van informatie door een SOC is noodzakelijk voor een volledig dreigingsbeeld, waarbij rekening gehouden moet worden met de belasting van het SOC-team.[20]

De risico's van complexiteit in de leverancierssketen binnen een operationele omgeving

Supply chain lijkt eenvoudig, maar is dat niet. In wezen betreft het de volledige keten van leveranciers van materialen en diensten voor productfabricage. Een supply chain omvat ERP (Enterprise Resource Planning), MES (Manufacturing Execution System), warehouse management, logistiek, distributie, ploegendienstplanning, en materiaal bestel- en leveringsprocessen. Het betreft een ecosysteem van partijen die onderdelen, grondstoffen, software, hardware, digitale diensten, applicaties, cloudtoepassingen, webservices, enzovoorts leveren, onderhouden, distribueren en opslaan.

Wat heeft dit met cybersecurity te maken? Moderne auto's bevatten veel rekenkracht en chips van gespecialiseerde bedrijven. Om de cybersecurity van een auto te waarborgen, moeten zowel de autofabrikant als de toeleveranciers voldoen aan dezelfde beveiligingseisen. Tegenwoordig communiceren auto's met een back-end bij de fabrikant, wat communicatie tussen auto en eigenaar mogelijk maakt. Om te voldoen aan de UNECE R-155 regels voor het leveren van auto's in Europa, moet de autofabrikant aantonen dat de supply chain, fabriek en bedrijfsvoering cyberveilig zijn.

Een ander bekend voorbeeld is het intentionele vermijden van Huawei als leverancier van hard- en software ten behoeve van core telecom- en internetnetwerk infrastructuur door providers in Nederland. Men vindt de kans op onzuivere praktijken door het bedrijf te risicovol voor het inzetten van apparatuur in primaire (inter) nationale communicatiediensten.

De energietransitie introduceert nog een mogelijkheid voor zonnepaneel- en omvormer fabrikanten, die staan vaak rechtstreeks in verbinding met een webportal van de fabrikant. Als die producent ook toegang heeft om commando's uit te voeren op de omvormer kan in theorie in één klap een deel van de zonnestroom uitvallen. Wat grote consequenties kan hebben voor de elektriciteitsnetwerken.

Een supply chain omvat ERP (Enterprise Resource Planning), MES (Manufacturing Execution System), warehouse management, logistiek, distributie, ploegendienstplanning, en materiaal bestel- en leveringsprocessen.

[13] https://www.infosecurity-magazine.com/news/russian-malware-threat-energy-grids/
[14] https://www.nozominetworks.com/blog/mitigating-the-potential-impact-of-covid-19-related-ot-security-risks
[15] https://www.techtarget.com/iotagenda/definition/Indu¬¬strial-Internet-of-Things-IIoT
[16] https://claroty.com/blog/ics-security-the-purdue-model
[17] https://www.securitymetrics.com/blog/wireless-access-point-protection-finding-rogue-wi-fi-networks
[18] https://www.cybertalk.org/2024/06/28/10-daunting-cyber-physical-attacks-and-proactive-mitigations/
[19] https://www.nozominetworks.com/blog/open-drone-id-nozomi-networks-adds-support-to-detect-drones-with-guardian-air
[20] https://www.ictmagazine.nl/nieuws/minder-grip-op-cybersecurity-door-groot-aantal-alerts/

Afbeelding 2: *OT-misvattingen*

Vaak voorkomende misvattingen/ mythes ten opzichte van OT

- Alles waarin Windows of Linux OS draait hoort bij de Enterprise ICT afdeling
- Het gaat om IT-achtige end-points met specifieke software
- Het zijn maar weinig apparaten in vergelijking met IT-omgeving
- Zero-trust technieken kan alle sores qua OT security oplossen
- IT security scanning tools brengen alles van de OT-omgeving in zicht
- Cyberbeveiliging is alleen nodig om de grens tussen OT en IT te bewaken
- Internet connectiviteit richting de OT-omgeving is nooit gewenst
- Bedrijfsprocessen kunnen het best off-site - in de cloud of in centrale datacenter – gehost worden
- Medewerkers loggen altijd in met persoonlijke inlog gegevens
- Beheerders van de OT-omgeving snappen IT security beleid niet
- OT-omgeving vormt een risico voor de IT-omgeving – niet andersom
- IT-omgeving is perfect beveiligd en dus vormt geen risico voor de OT-omgeving

Waarom is een goed geregeld asset management van belang binnen OT?

Verantwoordelijkheden voor OT-installaties zijn zelden voldoende vastgesteld. Stakeholders kunnen in meerdere categorieën. Zie afbeelding 3.

Voor beschikbaarheid, betrouwbaarheid, veiligheid en cyberbeveiliging van een OT-omgeving is samenwerking tussen alle stakeholders essentieel. Zoals het volgen van een gezamenlijke onderhoudskalender om uptime te maximaliseren.

Afbeelding 3: *Stakeholder Categorieën*

Categorie	Voorbeelden
Gebruikers	Fabriekshoofd; Chef van dienst; shiftlead; operator Productiemanager
Onderhoudsploeg	Monteur; applicatie beheerder; leverancier; buitendienst operator
Geldverstrekkers	Productiemanager; CFO
Anderen	R&D; innovatie; CISO; kwaliteitscontrole, interne audit

Afbeelding 4 illustreert tegelijkertijd de enorme diversiteit aan leveranciers en partners betrokken kunnen zijn. Het geïntegreerde systeem kan dus heel complex zijn. Als het eenmaal getest, opgeleverd en volledig operationeel is, is er een immense druk om zo'n proces niet te storen – niet door cyber aanvallen – maar ook niet om kritische cyber updates te installeren.

Proactief OT-security met NIS2

De NIS2 (Network and Information Security 2) richtlijn, is een Europese wetgeving over cyberveiligheid.[21] Deze wetgeving verplicht organisaties om maatregelen te treffen om het algemene niveau van cyberbeveiliging in Europa te verhogen.

Van Europese richtlijn tot nationale wetgeving

Sinds januari 2023, werkt de Nederlandse overheid aan de vertalingsslag van de verplichte NIS2 richtlijn voor alle lidstaten naar nationale wetgeving. Dit is een complex proces, omdat het een grote impact zal hebben voor Nederlandse organisaties. Zo zullen steeds meer organisaties gevraagd worden om compliant te worden, zoals de Wbni. Dit betekent dat er meer sectoren aan de wetgeving dienen te voldoen. Dit brengt niet alleen diverse uitdagingen voor organisaties in Nederland met zich mee, maar ook voor de overheid, die verantwoordelijk is voor de implementatie, informatievoorziening, advisering en handhaving van de nieuwe wet. Organisaties die aan deze wetgeving moeten voldoen, zullen meer moeten doen om hun cyberbeveiliging te versterken en processen te beschermen tegen cyberdreigingen.

Welke sectoren is de wetgeving NIS2 van toepassing?

De NIS2 richtlijn is van toepassing op sectoren en organisaties die van vitaal belang zijn. Onder vitaal, wordt verstaan dat bij uitval van de processen de kans reëel aanwezig is voor maatschappelijke ontwrichting. De beoordeling of een proces of een dienst vitaal is, wordt gemaakt door het verantwoordelijke ministerie. Hierbij wordt geanalyseerd of er bij een incident dermate ernstige gevolgen kunnen optreden, dat

deze de nationale veiligheid kunnen schaden. Het NCSC (Nationaal Cyber Security Centrum) verdeelt sectoren die vitaal van belang zijn voor Nederland als: zeer kritieke sectoren en andere kritieke sectoren. Zie afbeelding 5 voor kritieke sectoren.

Proactief OT-security met NIS2

De NIS2 (Network and Information Security 2) richtlijn, is een Europese wetgeving over cyberveiligheid[21]. Deze wetgeving verplicht organisaties om maatregelen te treffen om het algemene niveau van cyberbeveiliging in Europa te verhogen.

Afbeelding 4:
Diversiteit van OT end-points.

Diversiteit van OT end-points is enorm – denk aan:

Hand scanners, Autonomous guided vehicles, robot installaties, hijskranen, lopende banden, RF-ID sensoren, peil meters, kwaliteits-sensoren, product tellers, condition based monitoring sensoren, slijtage sensoren, bedieningspanelen (HMI), energie meters, controle kamer workstations, infobeeldschermen, engineering workstations/ laptops, remote desktop oplossingen, RF-ID lezers, camera's, optische sensoren, augmented realiteit middelen, industriële gereedschap, coördinaat meetapparatuur, vuur en gas sensoren, noodstop mechanisme, lucht kwaliteitsmeter, pompen, afsluiters, label printers enz

Afbeelding 5:
Kritieke sectoren

Zeer kritieke sectoren:

Energie, transport, infrastructuur financiële markt, gezondheidszorg, drinkwater, digitale infrastructuur, afvalwater, overheidsdiensten, ruimtevaart, beheerders van ICT-diensten en bankwezen.

Andere kritieke sectoren:

Digitale aanbieders, post- en koeriersdiensten, afvalstoffenbeheer, levensmiddelen, chemische stoffen, onderzoek, vervaardiging en manufacturing.

De wettelijke eisen onder NIS2- richtlijn?

De wetgeving NIS2 vereist het inrichten van processen ten behoeve van nieuwe cybersecurity verantwoordelijkheden, namelijk: zorgplicht, meldplicht, registratieplicht en rekening houden met controle en toezicht[23].

Zorgplicht

Organisaties worden verplicht om een risicoanalyse uit te voeren, op basis waarvan zij passende en evenredige maatregelen treffen voor de beveiliging van de interne netwerk- en informatiesystemen.

Meldplicht

De wetgeving vereist dat significante (cyber) incident(en) binnen 24 gemeld worden bij het Computer Security Incident Response Team (CSIRT) en het NCSC. Het gaat met name om incident(en) die de verlening van de diensten aanzienlijk verstoren. CSIRT zal vervolgens advies geven en waar nodig bijstand verlenen.

Registratieplicht

Organisaties die onder NIS2 vallen, moeten zich wettelijk registreren in het entiteitenregister. Het NCSC biedt een online registratievoorziening waarin organisaties zichzelf moeten aanmelden als NIS2-entiteit. Omdat deze registratie verplicht is voor alle EU-lidstaten, ontstaat uiteindelijk een overzicht van trends en ontwikkelingen rond dreigingen en incidenten binnen de lidstaten.

Toezicht

Organisaties die onder de wetgeving vallen zijn onderworpen aan toezicht zoals de zorg- en meldplicht door de nationale overheid. Het toezicht richt zich met name tot de entiteit, maar kunnen in bepaalde gevallen ook individuele bestuurders van organisatie raken.

Wat betekend implementatie van NIS2 voor uw organisatie?

De organisaties die onder NIS2 vallen, moeten maatregelen treffen om hun netwerk- en informatiesystemen te beschermen tegen incidenten. Dit geldt ook voor de fysieke omgeving waarin de systemen zich bevinden. In afbeelding 6 worden tien zorgplicht maatregelen gedefinieerd die organisaties moeten regelen om NIS2 compliance te kunnen zijn.[24]

Afbeelding 6: *Tien Zorgmaatregelen*

Maatregel 1:
Een risicoanalyse en beveiliging van informatiesystemen

Maatregel 2:
Beveiligingsaspecten op het gebied van personeel, toegangsbeleid en beheer van assets

Maatregel 3:
Maatregel op het gebied van bedrijf continuïteit, zoals back-up beheer en noodvoorzieningenplannen

Maatregel 4:
proces voor incidentmanagement.

Maatregel 5:
Awareness creëren onder medewerkers en andere

Maatregel 6:
Tien zorgplichtmaatregelen

Maatregel 7:
Beveiliging van de toeleverancierskete

Maatregel 8:
Beleid en procedures over het gebruik van cryptografie en encryptie

Maatregel 9:
het gebruik van Multi Factor Authenticatie (MFA), beveiligde spraak- video- en tekstcommunicatie en beveiligde noodcommunicatiesystemen

Maatregel 10:
beleid en procedures om de effectiviteit van beheersmaatregelen van cyberbeveiligingsrisico's te beoordelen.

De toekomst en verwachtingen

IT en OT komen steeds dichterbij elkaar, zowel qua technologie als integratie. Dit vergroot de functionele mogelijkheden, maar ook de aanvalsexposure en impact. Wanneer alles met elkaar verbonden is, kan een klein foutje een sneeuwbaleffect veroorzaken zonder goede processen en maatregelen. Organisaties worden zich langzaam bewust van de gevolgen van de digitale wereld. Het opzetten van effectieve maatregelen en bijbehorende processen vereist tijd, inspanning en doorzettingsvermogen. Deze inspanningen moeten worden ondersteund door het hoogste management om de weerbaarheid van organisaties tegen huidige en toekomstige cyberaanvallen te vergroten.

[21] https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32022L2555
[22] https://www.ncsc.nl/over-ncsc/wettelijke-taak/wat-gaat-de-nis2-richtlijn-betekenen-voor-uw-organisatie/valt-uw-organisatie-onder-de-cer-en-nis2-richtlijnen
[23] https://www.ncsc.nl/over-ncsc/wettelijke-taak/wat-gaat-de-nis2-richtlijn-betekenen-voor-uw-organisatie/samenvatting-nis2-richtlijn
[24] https://www.digitaltrustcenter.nl/nis2/startpunt#10maatregelen

Over de auteurs:

Cathy Ellis

OT Cybersecurity Specialist

Cathy is sinds 2011 OT infra- en securityarchitect. Met haar achtergrond in elektrotechniek, telecom en netwerkontwerp kan ze cybersecurityvraagstukken in industriële, proces- en operationele omgevingen aanpakken. Ze werkt nu aan het overbrengen van kennis en kunde uit de energie-industrie naar de logistiek- en transportsector.

www.linkedin.com/in/cathellis/

cathy.ellis@capgemini.com

Martijn Grootenboer

OT Security consultant

Martijn helpt klanten met het beoordelen en beveiligen van OT omgevingen en trainen van personeel.

www.linkedin.com/in/ing-martijn-grootenboer/

martijn.grootenboer@capgemini.com

Rafik Nasiri

Cybersecurity & Privacy consultant

Rafik is een Cybersecurity en privacy consultant die actief is voor verschillende nationaal als internationale organisaties met uiteenlopende vragen omtrent cybersecurity en privacy vraagstukken.

www.linkedin.com/in/rafik-nasiri-9b9b64a9/

rafik.nasiri@capgemini.com

03

Generatieve AI: het mes snijdt aan twee kanten voor Cybersecurity

Wat zijn de voordelen, risico's en bedreigingen van generatieve AI voor de cyberbeveiliging van een organisatie?

Highlights

- Door GenAI zijn technieken als phishing, deepfakes en social engineering-aanvallen niet van echt te onderscheiden. Generatieve AI kan phishing, deepfakes en social engineering aanvallen aanzienlijk verbeteren door zeer overtuigende en gepersonaliseerde berichten te creëren. Dit vormt een bedreiging voor het vertrouwen in de authenticiteit van digitale communicatie.
- Automatisering van security en beleid: GenAI kan de efficiëntie verbeteren door het automatiseren van patchbeheer en het opstellen van beveiligingsbeleid.
- Proactief onderzoek naar dreigingen en verbeterde incidentrespons worden effectiever dankzij GenAI's vermogen om grote datasets te analyseren en realtime dreigingsinformatie te genereren. Dit is gunstig voor het SOC/SIEM van bedrijven.

Generatieve AI (GenAI) bevindt zich momenteel in de overgangsfase van een technologische hype naar een zakelijke tool die daadwerkelijk waarde toevoegt. Nu bedrijven GenAI in toenemende mate gebruiken om hun productiviteit en efficiëntie te verhogen, is het belangrijk om zowel de voordelen als de valkuilen te begrijpen in de context van cyberbeveiliging. In dit artikel onderzoeken we hoe beveiligingsteams kunnen profiteren van GenAI maar ook hoe de technologie kan worden misbruikt. We belichten de bekende beveiligingsrisico's die iedere organisatie in haar strategie zou moeten opnemen.

Spam e-mails zullen minder 'phishy' lijken

Het herkennen van een spam e-mail is voor veel mensen al een uitdaging, en dat zal de komende jaren alleen maar lastiger worden. Phishing-e-mails zijn nu nog vaak te herkennen aan spelfouten of vreemde zinsconstructies. Large Language Models (LLM's) maken phishing e-mails (helaas) steeds overtuigender. Deze modellen kunnen specifieke, overtuigende en grammaticaal correcte e-mails schrijven, aangepast aan de interesses van een specifiek persoon. De mails worden geloofwaardig door de overtuigende toon, schrijfstijl en grammaticaal correcte inhoud.

Dankzij GenAI kunnen cybercriminelen kunnen phishing e-mails van extreem hoge kwaliteit produceren en zo hun slagingskans bij potentiële slachtoffers vergroten. Als input kunnen ze openbaar beschikbare informatie gebruiken om gepersonaliseerde berichten voor gerichte aanvallen te ontwikkelen. Daarnaast kunnen e-mailsjablonen en visuele hulpmiddelen die officiële communicatie nabootsen, gemakkelijk worden gegenereerd met behulp van codetools.

De combinatie van gepersonaliseerde berichten en het steeds correctere taalgebruik en grammatica draagt bij aan de toenemende dreiging van

phishing. Het is dan ook essentieel om goed functionerende detectie- en preventietools in te zetten die phishing e-mails te kunnen tegenhouden, net als het continu trainen van medewerkers op het terrein van nieuwe phishingdreigingen.

Realistische deepfakes en social engineering

GenAI kan inmiddels ook realistische media, zoals stem- en videofragmenten ontwikkelen. Cybercriminelen kunnen daarmee de stem van allerlei personen nabootsen of nep (live) videobeelden genereren en hiermee social engineering aanvallen uitvoeren. Grote kans dat potentiële slachtoffers zich niet realiseren dat de persoon met wie ze communiceren geen collega, vriend of familielid is, maar een cybercrimineel die voldoende gegevens heeft verzameld om ze te overtuigen hun vertrouwelijke informatie te delen of transacties uit te voeren.

GenAI verandert ook de manier waarop malware wordt geproduceerd. Dankzij GenAI wordt het voor cybercriminelen veel eenvoudiger om gevaarlijke software te maken en te verspreiden.

De opkomst van deze social engineering-aanvallen is buitengewoon moeilijk te bestrijden. Dat vereist van werknemers om hun openbare gegevens te beperken en hoge privacy- en beschermingsstandaarden te gebruiken. Zo zouden werknemers veel meer en vaker verificatievragen moeten stellen over recente interacties met collega's, specifieke projectdetails of andere niet-openbare informatie.

Het is cruciaal om bewustwording te creëren over de nieuwe tactieken. Het opstellen van verificatievragen voor communicatie kan een nuttige methode zijn om de authenticiteit van de persoon te verifiëren. Identificeer de gevoelige communicatiekanalen en ontwikkel verificatievragen die alleen de legitieme partijen kennen.

Malware genereren: toegankelijk voor iedereen

GenAI verandert ook de manier waarop malware wordt geproduceerd. Dankzij GenAI wordt het voor cybercriminelen veel eenvoudiger om gevaarlijke software te maken en te verspreiden. Generatieve modellen kunnen onder meer worden gebruikt om nieuwe soorten malware te creëren, die zich continu aanpassen en detectiesystemen - bijvoorbeeld op handtekeningen gebaseerde antivirus-systemen - ontwijken. Als cybercrimineel heb je nauwelijks nog technische drempels. Dat vergroot de kans op geavanceerde malware-aanvallen aanzienlijk.

Bovendien kan GenAI worden ingezet om grote opensourcecode-opslagplaatsen te doorzoeken op zero-day aanvallen en eerdere kwetsbaarheden te ontdekken of om verdedigingssystemen te omzeilen. Naarmate de generatieve modellen verder verbeteren, wordt verwacht dat ook het ontwikkelen van malware zal toenemen evenals de effectiviteit van dergelijke aanvallen.

Op gedraggebaseerde systemen worden cruciaal in de strijd tegen de opkomst van nieuwe malware. Door gegenereerde malwaremodellen te gebruiken voor training kunnen deze defensieve beveiligingssystemen hun detectiemogelijkheden verbeteren. Het is zeer waarschijnlijk dat er een GenAI-wapenwedloop gaat ontstaan tussen enerzijds het genereren van malware en anderzijds het detecteren en de preventie van malware. Vroeg of laat zal dat ook voor organisaties betekenen dat ze zich moeten 'bewapenen' met GenAI-verdedigingsmogelijkheden. Er zijn nu al goede tools beschikbaar binnen de diensten van de grotere cloudserviceproviders en hyperscalers als basis voor een GenAI-verdediging van uw organisatie.

Zwakke punten van LLM's

Het is algemeen bekend dat LLM's gevoelig zijn voor SQL injection attacks. Bij SQL injection attacks is sprake van kwaadwillend gegenereerde input die voor een LLM een geloofwaardige instructie lijkt. Dit wordt vaak gebruikt in combinatie met jailbreaken, een methode om de beveiliging van het model uit te schakelen. De meest voorkomende gevolgen van SQL injection attacks zijn onder meer gegevensdiefstal, het verspreiden van verkeerde informatie, bevooroordeelde informatie en het uitvoeren van kwaadaardige code.

Dit soort aanvallen kent twee categorieën. Bij aanvallen met SQL injection attacks (1) wordt het model expliciet om gegevens gevraagd zoals persoonlijke gegevens of gevoelige informatie zoals API-sleutels (Application Programming Interface). Hier is het model doorgaans niet voor ontworpen. Bij indirecte aanvallen (2) wordt de malware ingebed in de inhoud die door de modellen wordt gebruikt, zoals webpagina's of codeopslagplaatsen. Deze aanvallen kunnen desinformatie opleveren, waardoor de betrouwbaarheid van het model afneemt.

Het herkennen van een spam e-mail is voor veel mensen al een uitdaging, en dat zal de komende jaren alleen maar lastiger worden.

Het beschermen van modellen tegen dit soort SQL injection attacks vereist een combinatie van maatregelen. Denk daarbij aan voldoende invoervalidatie, autorisatiecontroles gekoppeld aan specifieke informatie, snelle validatie van de context die wordt gemanipuleerd en continue monitoring van het model. Er bestaat echter niet één oplossing die het probleem voor alle modellen op uniforme wijze oplost, omdat dat inherent is aan de manier waarop LLM's functioneren. Naarmate de modellen verbeteren, wordt verwacht dat er tijdens het trainen van medewerkers meer vijandige scenario's worden geïntroduceerd om de modellen veerkrachtiger te maken tegen SQL injection attacks.

Beveiligingspreventie versterken met GenAI

De eerste fase van het beveiligen van een digitale omgeving bestaat uit het introduceren van preventieve maatregelen die de kans op aanvallen verkleinen, het systeem bestand maken tegen verwachte aanvallen én beveiligingsrichtlijnen en -beleid vaststellen. GenAI kan een belangrijke rol spelen bij het automatiseren van security door codebases te scannen op kwetsbaarheden en passende maatregelen te stellen. Dat is essentieel voor zowel open-sourcetools als actieve codebases die door ontwikkelaars worden onderhouden, waardoor veilige softwareontwikkelingspraktijken worden vergemakkelijkt.

Bovendien kan GenAI helpen bij het opstellen van een beveiligingsbeleid. GenAI kan verschillende versies van raamwerken of richtlijnen die binnen het beleid worden gebruikt met elkaar vergelijken, de verschillen samenvatten en de kennis samenvoegen in een format dat vervolgens ook geschikt is voor beleidsupdates. Dat maakt het eenvoudiger om het up-to-date houden van het beveiligingsbeleid te stroomlijnen en zorgt ervoor dat de nieuwste ontwikkelingen worden meegenomen.

Verbeterde detectie en respons

GenAI zal de komende jaren ook steeds belangrijker worden bij het versterken van de incidentdetectie- en responsmogelijkheden van beveiligingsteams. Beveiligingsteams

kunnen LLM's gebruiken om binnen enkele seconden informatie uit een heel landschap van logboeken en gebeurtenissen samen te vatten, op te vragen en te analyseren. Dit zorgt niet alleen voor de identificatie van huidige dreigingen, maar ook voor de detectie van dreigingen uit het verleden die mogelijk onopgemerkt zijn gebleven. Door het arbeidsintensieve logproces dat doorgaans gebruikt wordt door SOC-analisten te stroomlijnen, stellen LLM's analisten in staat zich te concentreren op de belangrijkste en meest opvallende gebeurtenissen die door AI worden geïdentificeerd.

GenAI is ook in te zetten bij het genereren van informatie over dreigingen. Zo kan het gegevens over Indicators of Compromise (IOC's) van het dark web, sociale media en andere beveiligingsfeeds halen en direct realtime lijsten van IOC's produceren. Automatisering in combinatie met generatieve modellen kan draaiboeken creëren. Deze draaiboeken kunnen herstel- en responsacties bij gedetecteerde bedreigingen automatiseren, denk aan het automatisch bijwerken van blacklists.

Bovendien kan generatieve AI worden gebruikt voor het opsporen van bedreigingen. Zo kunnen analisten ultrasnel zoeken naar cyberbedreigingen die anders mogelijk onopgemerkt hadden kunnen blijven. Daarvoor kunnen ze bijvoorbeeld vragen genereren basis van hypothetische scenario's en door grote datasets bevragen op relevante informatie.

Voorbereiden, aanpassen, beschermen

Nu we in een tijdperk zijn aanbeland waarin GenAI steeds meer is geïntegreerd in cyberbeveiliging, is het voor organisaties belangrijk om zowel de kansen als de uitdagingen die deze technologie biedt, voor te blijven. GenAI is twee zijden van dezelfde medaille. Het biedt aanzienlijke voordelen bij het automatiseren van taken, het verbeteren van de respons op incidenten en het verbeteren van beveiligingsmaatregelen. Maar het biedt ook nieuwe wegen waar cybercriminelen misbruik van kunnen (en zullen) maken. Door het dubbele karakter van deze technologie te begrijpen, kunnen beveiligingsteams hun strategieën beter voorbereiden ter bescherming tegen geavanceerde cyberdreigingen. Voortdurende training, streng cybersecuritybeleid en het voortdurend proactief opsporen van bedreigingen zullen in de komende jaren basaal blijken om de voordelen van GenAI te benutten en tegelijkertijd de risico's te beperken.

De toekomst van cyberbeveiliging ligt in het vinden van de balans tussen het benutten van innovatieve technologieën en het waakzaam blijven bij opkomende bedreigingen.

Over de auteurs:

Jean Smidt

Senior Security Consultant

Jean heeft een brede achtergrond in informatiebeveiliging, die zowel het testen, de engineering en architectuur omvat. Hij benut zijn ervaring op het gebied van informatiebeveiliging om raakvlakken te onderzoeken met opkomende onderwerpen zoals AI en cloudtechnologieën.

www.linkedin.com/in/jean-de-smidt/
jean.smidt@capgemini.com

Ruben Tienhooven

Stream Lead Cloud Security

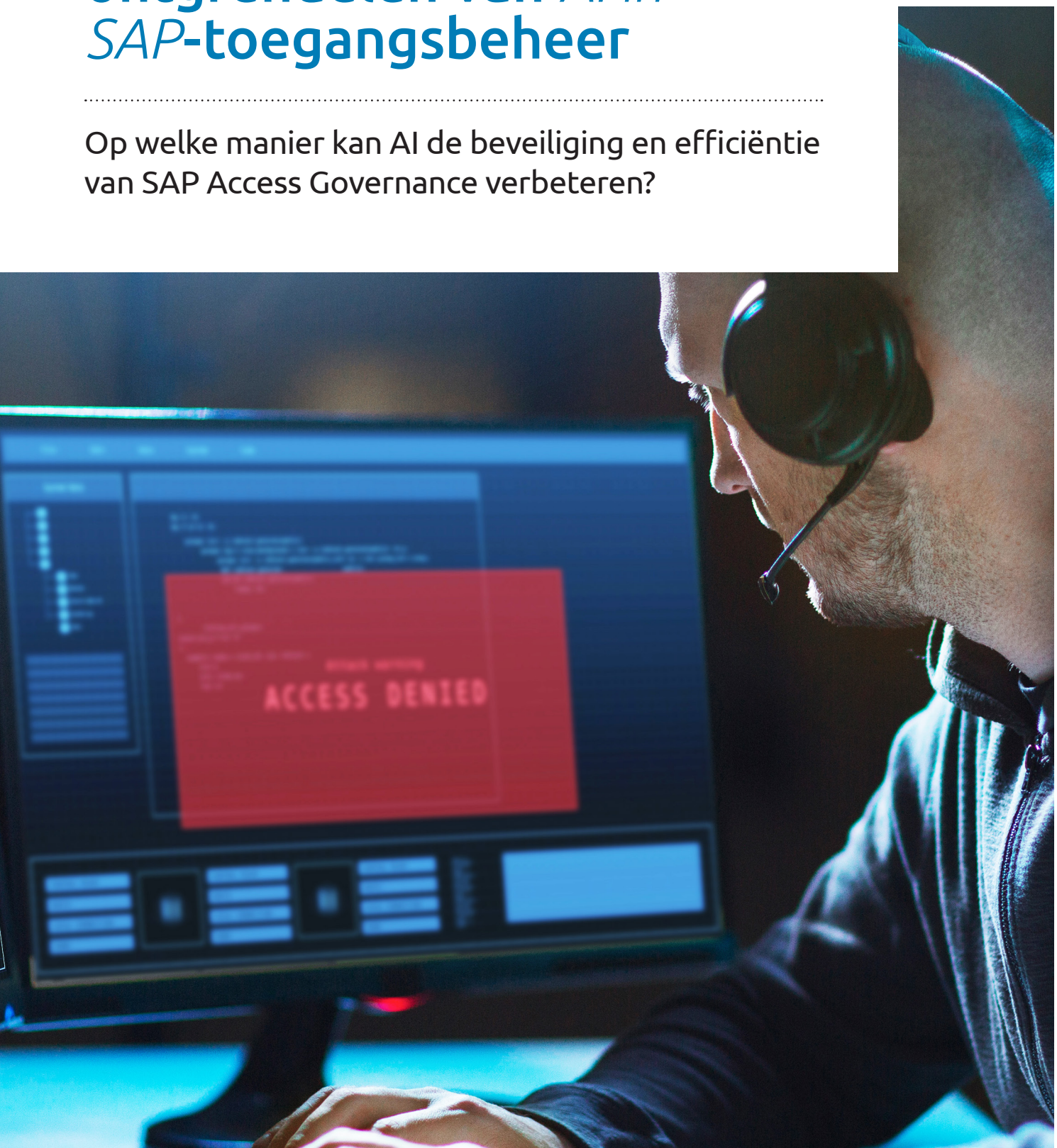
Als jurist en IT-specialist weet Ruben de twee werelden van het cyberdomein samen te brengen. In zijn werk weet Ruben de eisen van wetten, regelgeving en het bedrijfsleven te vertalen naar concrete acties en maatregelen die in de praktijk geïmplementeerd kunnen worden.

www.linkedin.com/in/rubentienhooven/
ruben.tienhooven@capgemini.com

04

De potentie ontgrendelen van *AI in SAP*-toegangsbeheer

Op welke manier kan AI de beveiliging en efficiëntie van SAP Access Governance verbeteren?



Highlights

- AI kan SAP Access Governance ondersteunen door geavanceerde beveiligings- en efficiëntiemaatregelen in te voeren.
- Traditionele methoden voor het beheren van SAP-toegang zijn vaak inefficiënt, foutgevoelig en kostbaar.
- Door AI aangedreven tools stroomlijnen de toelevering en compliance.
- Hoewel compliance noodzakelijk is, komt de kern van beveiliging voort uit proactieve en intelligente Access Governance strategieën.

SAP-systemen zijn cruciaal voor ondernemingen. Ze bevatten echter ook waardevolle data die cyberdreigingen aantrekken. SAP Access Governance gaat om de processen, tools en beleidsmaatregelen die worden gebruikt om de gebruikerstoegang tot SAP-systemen en -data te beheren en te controleren. Optimale Access Governance is niet alleen essentieel voor compliance, maar voor de algehele beveiliging. Kunstmatige Intelligentie (AI) kan SAP Access Governance ondersteunen door de beveiliging, efficiëntie en compliance te verbeteren Dit artikel gaat in op de mogelijkheden van AI om toegangsbeheer en bijbehorende vertrouwelijke informatie te transformeren en uw organisatie beter te beveiligen.

Uitdagingen in traditionele SAP Access Governance

In het huidige zakelijke landschap beheren SAP ERP-systemen alles: van financiën en human resources tot supply chains en klantrelaties. Deze systemen bevatten enorme hoeveelheden gevoelige en kritieke data, en dat vereist een complexe access governance. SAP Access Governance kent een uitgebreide set beleidsmaatregelen, procedures en technologieën die ontworpen is om de gebruikersrechten binnen SAP-omgevingen te beheren. Dit zorgt ervoor dat alleen geautoriseerde personen specifieke informatie kunnen inzien en functies kunnen uitvoeren. Dat vermindert het risico op datalekken, fraude en operationele verstoringen.

Traditionele SAP Access Governance vereist echter ook een aanzienlijk aantal handmatige handelingen om de gebruikersrechten te beheren en te monitoren om veiligheid en compliance te waarborgen.

Dat brengt verschillende beperkingen met zich mee:

- **Inefficiëntie:** Handmatige processen nodig voor het toewijzen, beoordelen en intrekken van toegangsrechten zijn tijdrovend en arbeidsintensief. Deze inefficiëntie vertraagt de bedrijfsvoering en vermindert de algehele productiviteit.
- **Foutgevoeligheid:** Menselijke fouten vormen een significant risico. Fouten bij het toewijzen van toegangsrechten of het niet tijdig bijwerken ervan kunnen leiden tot ongeautoriseerde toegang of onvoldoende rechten, waardoor de veiligheid en compliance in gevaar komen.
- **Hoge kosten:** Het handmatig beheren van toegangsrechten vereist aanzienlijke menselijke arbeid. Organisaties moeten namelijk voortdurend investeren in gekwalificeerd personeel om deze taken uit te voeren. Dit leidt tot verhoogde operationele kosten.
- **Toegenomen complexiteit:** Naarmate organisaties groeien en nieuwe diensten toevoegen aan hun bestaande IT-portfolio, neemt de complexiteit van het beheren van toegangsrechten toe. Dit maakt het nog moeilijker om accurate toegangscontroles te handhaven.
- **Naleving van regelgeving:** Het waarborgen van het naleven van vereisten zoals GDPR, SOX en HIPAA, vraagt om uitgebreide documentatie en rapportage. Traditionele methoden hebben moeite om aan deze eisen te voldoen, waardoor organisaties het risico lopen op non-compliance.

Voorbeelden:

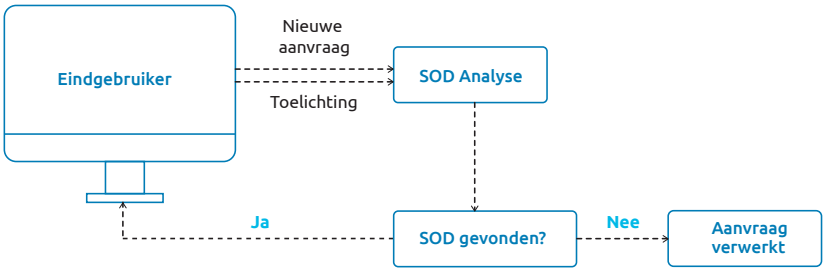
Use Case I:

SAP heeft een tool genaamd SAP GRC (Governance, Risk and Compliance) die het access control (AC) proces kan automatiseren. Het SAP-autorisatieteam is normaal gesproken verantwoordelijk voor het AC-proces. Om veiligheid en compliance te waarborgen, wijst het SAP-autorisatieteam de gevraagde toegang toe. Dat beperkt de risico's tot een minimum. Hierbij worden twee specifieke AC-modules veelvuldig gebruikt: SAP Access Request Management (ARM) en Access Risk Analysis (ARA). Elke toegangsaanvraag kent een risicobeoordelingsproces (ARA-module). Als een risico wordt geïdentificeerd, dan wordt de gebruiker gevraagd om een zakelijke rechtvaardiging te geven. Wordt de rechtvaardiging goedgekeurd door de systeembeheerder, dan wordt de toegangsaanvraag verwerkt (ARM-module).

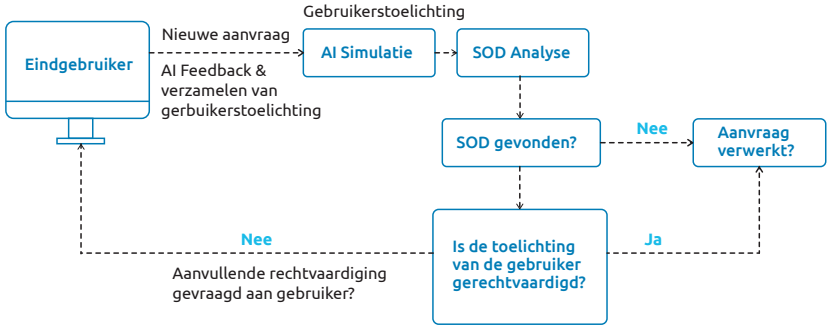
Als voorbeeld: tijdens de risicoanalyse worden Segregation of Duties (SoD)-risico's speciaal geanalyseerd door de autorisatieconsultant. Een SoD-risico verwijst naar de mogelijkheid van belangenconflicten en fraude die kan ontstaan wanneer een enkele persoon controle heeft over meerdere stadia van een kritisch bedrijfsproces. Denk aan een gebruiker die toegang vraagt om zowel een factuur aan te maken als goed te keuren. Als toegang wordt verleend, kan die gebruiker ook frauduleuze facturen genereren en goedkeuren. In dit scenario zal het beveiligingsteam daarom eerst een SoD-analyse uitvoeren en het risico markeren. Het beveiligingsteam neemt vervolgens contact op met de gebruiker om aan te geven waarom toegang nodig is. (afbeelding 1)

Wanneer AI wordt ingezet, dan kan een gebruiker direct bij het aanmaken van de toegangsaanvraag een simulatie van de potentiële risico's worden getoond (afbeelding 2). Dat geeft de aanvrager direct inzicht in de risico's. AI kan gebruikers dus helpen de initiële aanvragen aan te passen met geminimaliseerde risico's om beter aan hun behoeften te voldoen. Daardoor hoeven er ook minder werknemers betrokken te worden bij het totale proces. Zelfs als de aanvrager specifieke toegang nodig heeft - en dat mogelijk een risico kan veroorzaken - kan AI informatie van de aanvrager verzamelen over de noodzaak voor de werkzaamheden voordat de aanvraag naar de toegangsverwerker wordt gestuurd. Dit vermindert het aantal menselijke handelingen en versnelt het proces van het verwerken van de aanvraag aanzienlijk.

Afbeelding 1: *Bestaand scenario*



Afbeelding 2: *voorgesteld scenario*



Use Case II:

De SAP GRC Access Control-oplossing kent Emergency Access Management (EAM) voor het afhandelen van dringende toegangsaanvragen. Dit proces hangt nu af van menselijke handelingen in meerdere stadia: eindgebruikers vragen toegang aan via het GRC-portaal en systeembeheerders verlenen goedkeuring op basis van zakelijke autorisatie. Daarna controleren reviewers vervolgens handmatig vijf verschillende logboeken op discrepanties en nemen contact op met gebruikers voor opheldering indien nodig.

Een AI-gedreven systeem kan dit proces stroomlijnen. Door al tijdens het aanvraagproces automatisch alternatieve mogelijkheden te presenteren, kan het helpen bij het formuleren van passende aanvragen, historische gedragingen van de aanvrager tonen, discrepanties realtime bijhouden en realtime autorisatie regelen en deze aan de reviewer presenteren. Dit zorgt voor een directe link tussen functionele behoeften en technische facilitering van het proces, waardoor er meer controle over veiligheid en naleving wordt geboden.

Voorgaande voorbeelden laten zien hoe AI kan helpen bij het vinden van discrepanties en het opstellen van documentatie zodat er aanzienlijk minder (menselijke) handelingen nodig zijn in het EAM-proces. AI monitort de logboeken en gebruikt natuurlijke taalverwerking (NLP) om direct te communiceren met aanvragers als de toepassing afwijkt van de initiële aanvraag. Reviewers ontvangen vervolgens alle details en autorisaties op één plek. Daardoor is het niet langer nodig om meerdere logboeken bij te houden. AI kan ook helpen bij het vaststellen van patronen in discrepanties. Dit helpt reviewers bij de besluitvorming.

AI-gedreven SAP Access Governance in de praktijk

We hebben een chatbot-oplossing geïmplementeerd die is ontworpen om de complexiteit van AI-gedreven SAP Access Governance te begeleiden. Deze oplossing versnelt de toegangstoewijzing, verhoogt de productiviteit en zorgt voor compliance met minimale privileges. Tegelijkertijd verminderen de risico's en operationele kosten aanzienlijk.

Omdat we in ons dagelijks werk gewend zijn aan één-op-één communicatie, kan het gebruik van een NLP-module met een AI-ondersteunde chatbot enorm helpen. Deze chatbot verbetert de bedrijfsproductiviteit aanmerkelijk; de toegangstoewijzing kost geen weken meer maar wordt gereduceerd tot minuten. Het vereenvoudigt ook het toegangsbeheer dankzij een uniforme interface, het verbetert de gebruikerservaring en verlaagt opleidingskosten. Als voorbeeld: een medewerker die toegang nodig heeft tot een nieuw systeem kan voortaan met de chatbot communiceren om zijn requirements toe te lichten. De chatbot geeft informatie over de stappen die nodig zijn om toegang aan te vragen en kan zelfs de aanvraag namens de medewerker indienen. Dat stroomlijnt het proces en elimineert vertragingen. Door toegangsaanvragen en goedkeuringen voor niet-kritieke toegang te automatiseren, integreert de chatbot naadloos in platforms zoals Azure. Dat zorgt voor compliant zoekopdrachten, bepaalt het juiste toegangsniveau voor gebruikers en optimaliseert workflows.

De mogelijkheden van de chatbot kunnen worden aangepast om compliance rapportages te ondersteunen door gegevens te analyseren en rapporten in een specifiek formaat te genereren. Als het compliance team bijvoorbeeld een rapport nodig heeft met details over toegangsrechten en potentiële risico's voor verschillende afdelingen, kan de chatbot deze informatie samenstellen en direct een geformatteerd rapport produceren dat klaar is voor beoordeling of audit.

De implementatie van bovenstaande voorbeelden begint bij een grondige beoordeling van de bestaande access governance processen en het identificeren van welke oplossing op maat kan worden aangepast aan de specifieke behoeften van de organisatie. Experts moeten vervolgens zorgen voor een naadloze integratie in de IT-infrastructuur, wat bijdraagt aan minimale verstoring van de werkprocessen en maximale efficiëntie.

Door uitgebreide training en doorlopende ondersteuning kunnen teams de chatbot effectief benutten. Daarbij zorgen continue monitoring en verbetering ervoor dat de oplossing meegroeit met het bedrijf en zich aanpast aan veranderende vereisten en beveiligingsuitdagingen.

Conclusie

AI transformeert SAP Access Governance door de mogelijkheden voor security, efficiëntie en compliance te verbeteren. Door monitoring te automatiseren, risico's te voorspellen en toegangsbeoordelingen te stroomlijnen, kunnen organisaties dankzij AI kritieke gegevens proactief beschermen. Maar organisaties moeten zich hierbij wel realiseren dat AI aanzienlijke maatwerkkennis en investeringen vereist. Dat vraagt om deskundige begeleiding en innovatieve tools. Zo kunnen bedrijven met succes AI-gedreven SAP Access Governance implementeren, waardevolle activa beschermen én zorgen voor robuuste en toekomstbestendige beveiligingssystemen. Hoewel compliance essentieel is, is echte beveiliging uiteindelijk het resultaat van proactieve en intelligente access governance-strategieën.

Over de auteurs:

Ankit Arya

SAP GRC Consultant

Ankit is een SAP Security- en GRC-consultant met 10 jaar ervaring in verschillende leidende adviesrollen met de nadruk op audit-, risico- en compliance management. Ankit ontwierp en implementeerde uitgebreide bedrijfsgestuurde beveiligingsmodellen voor verschillende SAP ERP-producten in overeenstemming met auditvereisten.

www.linkedin.com/in/ankitarya1103/

ankit.arya@capgemini.com

Yunus Ceyhan

OT Security consultant

Yunus werkt als cybersecurity consultant met een focus op SAP-cybersecurity en Identity and Access Management. Met zijn achtergrond in AI gaat hij de uitdagingen aan om cybersecurity naar een hoger niveau te tillen met behulp van AI-technologieën.

www.linkedin.com/in/yunus-emre-ceyhan-98b9a5129/

yunus.ceyhan@capgemini.com

Kriti Gourab Biswas

Senior SAP Security and GRC Consultant

Kriti is een gecertificeerde SAP Security en GRC Consultant met 8 jaar ervaring in SAP-beveiligingsontwerp, implementatie, onderhoud, probleemoplossing en kwetsbaarheidsbeheer. Hij heeft gewerkt met klanten uit verschillende domeinen, zoals de detailhandel, de reismarktplaats, de halfgeleiderindustrie, de hightechindustrie en de Big 4-firma.

www.linkedin.com/in/kriti-gourab-biswas/

Kriti.gourab.biswas@capgemini.com

05

Versterk je weerbaarheid: de rol van GenAI in het waarborgen van Naleving

Kan GenAI helpen de cyberweerbaarheid te versterken en om te voldoen aan de compliance eisen?

Highlights

- Operationele weerbaarheid: een uitgebreide aanpak om onverwachte gebeurtenissen te kunnen beheren.
- De rol van GenAI: verbetert operationele weerbaarheid en compliance.
- Regelgevingen: diverse wetten dragen wereldwijd bij aan digitale operationele weerbaarheid.
- Beleid en procedures: de sleutel(s) tot het beheren van IT-risico's en het waarborgen van weerbaarheid.
- GenAI in de praktijk: verbetert de weerbaarheid in diverse sectoren.

In het dynamische zakelijke landschap van vandaag de dag is operationele veerkracht cruciaal. Organisaties krijgen te maken met steeds meer juridische en regelgevende vereisten die van toepassing zijn op hun (IT-)omgevingen. Het beheren van compliance over multi-cloudomgevingen en raamwerken kan echter een uitdaging zijn. Handmatige werkzaamheden, verschillende IT controles en redundante tests zorgen ervoor dat waardevolle tijd en middelen onnodig verspild worden.

Door IT-controles op een gestructureerde manier in kaart te brengen en een up-to-date registratie bij te houden, kunnen organisaties efficiënt navigeren door een berg aan overlappende wetgevende vereisten. Deze manier van werken stroomlijnt inspanningen voor compliance, vermindert de kosten en verhoogt de algehele weerbaarheid van organisaties.

In dit artikel bespreken we hoe automatisering het risicobeheerproces binnen organisaties verandert en organisaties in staat stelt te gedijen in een onderling verbonden wereld.

In een tijdperk waarin het aantal cyberdreigingen toeneemt, de gevolgen van klimaatverandering steeds zichtbaarder worden, is operationele weerbaarheid van groot belang. Operationele weerbaarheid gaat niet alleen over het doorstaan van onverwachte gebeurtenissen, maar ook over het anticiperen op, voorbereiden op, reageren op en herstellen van dergelijke gebeurtenissen. Het betreft het vermogen van een organisatie om haar kernproducten en -diensten te blijven leveren, zelfs tijdens of na verstoringen.

Operationele weerbaarheid overstijgt traditioneel risicobeheer en bedrijfscontinuïteitsplanning. Het hanteert een holistische benadering die regelmatige risicoanalyses, continue monitoring en proactieve IT-maatregelen omvat om problemen te voorkomen voordat ze ontstaan. Deze elementen zijn essentieel voor het opbouwen van cyberweerbaarheid en het voorkomen van problemen bij de bron.

De opkomst van generatieve AI (GenAI) heeft het belang van operationele weerbaarheid exponentieel vergroot. GenAI-systemen zijn in staat om nieuwe inhoud te genereren, beslissingen te nemen en te leren van interacties en analyses. Deze capaciteit om te genereren en te leren maakt ze tot uiterst krachtige instrumenten, maar introduceert ook een nieuw niveau van complexiteit en onvoorspelbaarheid.

Organisaties krijgen te maken met steeds meer juridische en regelgevende vereisten die van toepassing zijn op hun (IT-) omgevingen.

Naarmate GenAI-systemen steeds meer geïntegreerd worden in de dagelijkse operaties, neemt het risico op verstoringen toe als deze systemen falen of onvoorspelbare acties uitvoeren. Deze paradigmaverschuiving vraagt om een zorgvuldig ontworpen raamwerk om de dillema's aan te pakken die zijn ontstaan door de implementatie van geavanceerde GenAI-systemen.

De integratie van GenAI in bedrijfsprocessen biedt enorme kansen, maar brengt ook aanzienlijke risico's met zich mee. Dit dwingt organisaties om hun operationele veerkracht te versterken. Organisaties worden geconfronteerd met een complex web van juridische en regelgevende eisen, vooral binnen hun beheerde IT-landschappen.

De automatisering van compliance-systemen met behulp van GenAI-tools is alleen haalbaar als organisaties al volledige controle hebben over hun compliance-processen. Door het beheersen van hun compliance-traject kunnen organisaties automatisering naadloos integreren, dit leidt tot verhoogde efficiëntie en nauwkeurigheid bij het naleven van regelgevende normen.

In het volgende gedeelte bespreken we bespreken hoe GenAI kan worden ingezet om een continue naleving van normen en wetgeving te garanderen binnen het dynamische en snel veranderende landschap van organisaties.

Regelgevingen rondom operationele weerbaarheid

In de afgelopen jaren hebben de regelgevende autoriteiten het belang van operationele weerbaarheid benadrukt door nieuwe cybersecurity wetten in te voeren of bestaande wetten bij te werken.

In de EU spelen regelgevingen zoals de Algemene Verordening Gegevensbescherming (AVG), de Richtlijn inzake netwerk- en informatiebeveiliging (NIS 2-richtlijn) en DORA (Digital Operational Resilience Act) een cruciale rol.

AVG richt zich op de bescherming van de privacy van persoonsgegevens en zorgt ervoor dat organisaties strenge maatregelen nemen om persoonlijke informatie te beveiligen. Intussen is het doel van de NIS 2-richtlijn om de beveiliging van netwerken en informatiesystemen in de lidstaten te verbeteren en een uniforme aanpak te bevorderen om cyberdreigingen aan te pakken. DORA streeft naar harmonisatie van digitale weerbaarheidsinspanningen binnen de EU, zodat financiële entiteiten ICT-gerelateerde verstoringen kunnen weerstaan en herstellen.

Hoewel deze regelgevingen in de kern verschillen, dragen ze gezamenlijk bij aan het versterken van de digitale operationele weerbaarheid wereldwijd. Door verschillende aspecten van gegevensbescherming, cyberbeveiliging en operationele continuïteit aan te pakken, zorgen deze kaders ervoor dat organisaties digitale risico's effectief kunnen beheren en beperken. Dit zal uiteindelijk de integriteit en stabiliteit van mondiale digitale infrastructuren beschermen.

Wanneer we de focus verleggen van een wereldwijd standpunt naar het niveau van de organisatie, wordt het belangrijk om de invloed van beleid en procedures op operationele veerkracht te onderzoeken.

Beleid en procedures in operationele weerbaarheid

Als het gaat om operationele weerbaarheid, zijn drie aspecten cruciaal:

1. Het belang van beleid en procedures.
2. De noodzaak van een voortdurend leer- en aanpassingsvermogen.
3. De mogelijke bijdrage van GenAI.

De integratie van GenAI in bedrijfsprocessen biedt enorme kansen, maar brengt ook aanzienlijke risico's met zich mee.

01

De rol van beleid en procedures in operationele weerbaarheid

Beleid en procedures vormen de ruggengraat van operationele weerbaarheid omdat ze een gestructureerde aanpak bieden om IT-risico's te beheren. Ze geven duidelijke richtlijnen voor (IT) processen en activiteiten binnen organisaties. Zo wordt consistentie en efficiëntie van IT-compliance gewaarborgd. Om operationele weerbaarheid te leveren, moeten organisaties ervoor zorgen dat ze verschillende aspecten hebben geregeld, waaronder:

- Risico's in de toeleveringsketen/ uitbestede functies en mitigerende maatregelen
- Incidentmanagementbeleid en het incidentproces
- Informatiebeveiliging, cyberbeveiliging en gegevens beschermende IT-controles
- Changemanagementprotocollen
- Crisisbeheer- en communicatieplannen

Laten we het beleid voor incidentbeheer als voorbeeld nemen. Dit beleid, mits het consequent wordt onderhouden en geactualiseerd, schetst de te volgen stappen bij een beveiligingsinbreuk. Dit leidt tot onmiddellijke actie, beperkt de schade en bevordert een snel herstel. Het is echter niet alleen belangrijk om dit beleid te hebben, maar ook om heldere procedures te hanteren, te implementeren, regelmatig te herzien, bij te werken om de effectiviteit te waarborgen.

Een voorbeeld hiervan is het datalek bij Equifax in 2017, waar een goed gedefinieerd incidentresponsbeleid de gevolgen van het lek had kunnen beperken. De persoonlijke informatie van miljoenen burgers uit de Verenigde Staten, het Verenigd Koninkrijk en Canada werd in gevaar gebracht, wat resulteerde in een van de meest omvangrijke gevallen van cybercriminaliteit gerelateerd aan identiteitsdiefstal.

Hackers wisten via een bedrijfsnetwerk toegang te krijgen tot interne servers en ontdekten gebruikersnamen en wachtwoorden die in niet-versleutelde tekst waren bewaard, waardoor ze ook toegang kregen tot de rest van het systeem. Gedurende meerdere maanden verzamelden ze onopgemerkt gegevens in gecodeerde vorm. Dit was mogelijk door het verzuim om het encryptiecertificaat van een beveiligingstool te vernieuwen. De inbreuk had een aanzienlijke invloed op de reputatie van het bedrijf en resulteerde uiteindelijk in een overeenkomst met de Amerikaanse Federal Trade Commission.

Een ander voorbeeld is de ransomware-aanval op Change Healthcare, onderdeel van Optum en eigendom van UnitedHealth Group, in 2024. Dit bedrijf biedt een veelgebruikt programma aan voor zorgaanbieders om klantbetalingen en verzekeringsclaims te beheren.

De aanvallers maakten medische dossiers buit die betrekking hadden op een aanzienlijk aantal Amerikanen, waaronder persoonlijke informatie, medische gegevens en gegevens over ziektekostenverzekeringen. Deze cyberaanval leidde tot storingen en vertragingen bij duizenden zorgverleners, wat resulteerde in bijna twee weken van verstoringen in de levering van medicijnen en medische zorg in het hele land. De aanval op Change Healthcare staat bekend als een van de grootste digitale diefstallen van medische dossiers in de VS, met onschatbare gevolgen voor miljoenen Amerikanen.

Een duidelijk omschreven beleid voor incidentrespons had het bedrijf in staat kunnen stellen om snel de getroffen systemen te isoleren, de verdere verspreiding van de ransomware te stoppen en een sneller herstel mogelijk te maken.

Deze twee voorbeelden benadrukken het belang van een goed gedefinieerd incidentresponsbeleid. In beide gevallen had een dergelijk beleid de gevolgen van de inbreuk kunnen beperken en bijgedragen aan sneller herstel.

02

Het belang van voortdurende leer- en aanpassingsvermogen

Cyberweerbaarheid betreft niet alleen de aanwezigheid van robuuste systemen en applicaties, maar ook het gedetailleerd formuleren van beleidsmaatregelen en procedures. Deze richtlijnen fungeren als een draaiboek voor organisaties, waarin de te volgen stappen bij verstoringen worden uiteengezet. Ze verschaffen heldere instructies over rollen, verantwoordelijkheden en taken, waardoor een gecoördineerde respons wordt gewaarborgd.

Gezien de zich ontwikkelende bedreigingen, is het van cruciaal belang dat organisaties hun beleid en procedures voortdurend herzien en bijwerken. Statische beleidsmaatregelen zijn niet toereikend, gezien het dynamische karakter van het IT-landschap en de daarmee gepaard gaande risico's.

Organisaties dienen een cultuur te omarmen waarin continue ontwikkeling en leren centraal staan, specifiek gericht op cyberweerbaarheid. Het is noodzakelijk om regelmatige audits uit te voeren om de effectiviteit van het huidige beleid en de procedures op het gebied van cyberbeveiliging te evalueren. Het leren van eerdere cyberincidenten en bijna-incidenten speelt een cruciale rol in dit proces.

Daarnaast is het voor organisaties van essentieel belang om op de hoogte te blijven van de nieuwste trends en bedreigingen op het gebied van cyberbeveiliging om zo hun beleid proactief te kunnen bijwerken en hun cyberweerbaarheid te versterken. Met de opkomst van thuiswerken zijn beleidslijnen omtrent veilige externe toegang steeds belangrijker geworden.

Organisaties kunnen hun cyberweerbaarheid verbeteren en potentiële cyberbedreigingen een stap voor blijven door een cultuur te bevorderen die gericht is op continue verbetering en leren. Een dergelijke proactieve benadering kan de impact van cyberincidenten aanzienlijk verminderen wanneer ze zich voordoen, wat zorgt voor een snel herstel en minimale verstoring van de operaties.

03

De rol van AI in operationele weerbaarheid

Als we de rol van AI in operationele weerbaarheid verkennen, is het belangrijk op te merken dat de effectiviteit van GenAI afhangt van de kwaliteit en relevantie van de data waarop het is getraind. Voor risicobeheer is de meest waardevolle gegevensbron de eigen informatie van een organisatie, omdat deze is afgestemd op haar operaties en risicoprofiel. Daarom is GenAI binnen risicobeheer het meest nuttig binnen volwassen (IT) organisaties met uitgebreide ervaring in gegevensverzameling en -beheer, vooral op het gebied van risicobeheer.

Als GenAI wordt opgeleid met de specifieke data van een organisatie, heeft het de mogelijkheid om grote hoeveelheden informatie te doorgronden, patronen te herkennen en inzichten te verschaffen die anders over het hoofd zouden worden gezien. Dit verbetert zowel het auditproces als de detectie van bedreigingen. Bovendien kan GenAI adaptief leren vergemakkelijken door verschillende risicoscenario's te simuleren, waardoor organisaties beter voorbereid zijn op potentiële bedreigingen.

Echter, het is belangrijk om te benadrukken dat het inzetten van GenAI niet betekent dat menselijk toezicht overbodig wordt. GenAI dient als een instrument dat de menselijke vaardigheden kan versterken, maar ze niet kan vervangen. Daarnaast is het van belang dat GenAI op een respectvolle manier wordt gebruikt met betrekking tot privacy en vertrouwelijkheid, vooral wanneer het gaat om gevoelige gegevens voor risicobeheer.

In de volgende sectie zullen we bespreken hoe GenAI kan bijdragen aan operationele weerbaarheid als het verantwoordelijk en effectief wordt gebruikt. Deze discussie zal de uitdagingen en ethische overwegingen met betrekking tot het gebruik van GenAI omvatten.

Hoe kan GenAI helpen bij het verbeteren van operationele weerbaarheid?

GenAI kan de operationele weerbaarheid van organisaties op verschillende manieren aanzienlijk verbeteren. In de financiële sector kunnen GenAI algoritmes nieuwe data genereren op basis van bestaande markttrends en economische indicatoren. Deze gegenereerde data kan ingezet worden voor scenario-analyse en risicomanagement, waardoor financiële instellingen zoals banken en investeringsfondsen zich kunnen wapenen tegen een breed scala aan mogelijke marktverstoringen en effectief kunnen handelen als deze zich voordoen.

Daarnaast kan GenAI routinematige taken zoals dataverwerking en rapportages automatiseren. In een productieomgeving kan het bijvoorbeeld het proces van het vastleggen van productiegegevens automatiseren. Dit vermindert de kans op menselijke fouten en stelt medewerkers in staat zich te richten op complexere taken zoals kwaliteitsbewaking en procesverbetering.

GenAI kan ook realtime inzichten en voorspellende analyses bieden. In een retailbedrijf kan het verkoopdata analyseren om potentiële tekorten aan voorraad te voorspellen en optimale herbevoorradingsstrategieën voor te stellen, waardoor organisaties potentiële operationele problemen proactief kunnen aanpakken.

Of het nu gaat om het voorspellen van beursontwikkelingen in de financiële sector, het automatiseren van gegevensinvoer in de productie of het optimaliseren van voorraadbeheer in de detailhandel, GenAI speelt een cruciale rol bij het verbeteren van operationele weerbaarheid, het waarborgen van bedrijfscontinuïteit en het verbeteren van de algehele prestaties. Deze praktische voorbeelden illustreren hoe GenAI in scenario's uit de praktijk kan worden toegepast om operationele weerbaarheid in verschillende sectoren te versterken.

Het belang van het beheersen van risico's door het gebruik van GenAI

Het is essentieel om de risico's te beheren die verbonden zijn aan het gebruik van GenAI, zowel voor compliance als voor operationele weerbaarheid. Hoewel GenAI talrijke transformatievoordelen biedt, introduceert het ook nieuwe risico's die organisaties moeten leren beheersen. Als voorbeeld, GenAI kan onvoorspelbare resultaten opleveren, wat kan leiden tot onverwachte uitkomsten. Stel je een financiële instelling voor die GenAI inzet voor het berekenen van kredietscores, de resultaten kunnen variëren en onvoorziene gevolgen hebben.

Hoewel GenAI de efficiëntie en nauwkeurigheid kan vergroten, kan het ook zorgen voor irrelevante conclusies of beslissingen nemen die moeilijk te rechtvaardigen zijn, waardoor regelgeving zoals de Fair Credit Reporting Act in de VS of de AVG in de EU wordt overtreden.

Zo zou GenAI in de gezondheidszorg kunnen worden gebruikt om de uitkomsten van patiënten te voorspellen of behandelingen aan te bevelen. Als deze AI-systemen echter niet goed worden gemanaged, kunnen ze foutieve voorspellingen of aanbevelingen doen, wat mogelijk kan leiden tot schade voor de patiënt en schendingen van regelgeving zoals HIPAA.

Het is daarom van cruciaal belang dat organisaties solide strategieën voor risicobeheer toepassen bij het inzetten van GenAI. Dit houdt in dat er uitgebreide risico-evaluaties worden uitgevoerd, duidelijke governance-structuren worden opgezet en AI-systemen continu worden gecontroleerd om te garanderen dat ze functioneren zoals bedoeld en voldoen aan alle toepasselijke wet- en regelgeving. Op deze manier kunnen organisaties profiteren van de mogelijkheden van GenAI, terwijl ze tegelijkertijd compliance en operationele veerkracht waarborgen.

GenAI kan de operationele weerbaarheid van organisaties op verschillende manieren aanzienlijk verbeteren.

Conclusie

Operationele veerkracht is een veelzijdig concept dat een holistische aanpak vereist, inclusief zorgvuldig opgesteld beleid en procedures, continu leren en aanpassingsvermogen. De integratie van GenAI in bedrijfsprocessen brengt zowel enorme kansen als risico's met zich mee.

Hoewel GenAI de operationele veerkracht aanzienlijk kan vergroten door taken te automatiseren en real-time inzichten te bieden, brengt het ook nieuwe complexiteiten met zich mee die organisaties moeten zien te beheersen. Daarom is een grondige aanpak nodig die de kansen van GenAI combineert met risicobeheerstrategieën en daarbij menselijk toezicht cruciaal stelt. Alleen deze aanpak zal organisaties in staat stellen de voordelen van GenAI te benutten, compliance te handhaven en de operationele veerkracht in het dynamische zakelijke landschap te vergroten.

Over de auteurs:

Rahul Rauniyar

Senior Managing consultant: Security & Compliance Management

Rahul richt zich vooral op het implementeren en versnellen van compliance-automatisering, met een speciale focus op DORA, NIS2 en GenAI. In zijn rol bepaalt hij strategieën, beheert hij risico's en zorgt hij ervoor dat de IT-activiteiten van zijn organisatie voldoen aan het voortdurend veranderende compliancelandschap.

www.linkedin.com/in/rahul-rauniyar/
rahul.rauniyar@capgemini.com

Vera Irmak

Voormalig Privacy Consultant

Vera is een privacyprofessional met een gedegen juridische achtergrond. Ze richt zich op GDPR, de AI Act en naleving van cyberbeveiliging.

www.linkedin.com/in/verairmak0/

06

De Toekomst van *Digitale Identiteit* in Europa

Is de EUDI Wallet een zegen of een bedreiging voor de samenleving?

Highlights

- We beschrijven de trends en ontwikkelingen die aantonen waarom de EUDI Wallet belangrijk is voor burgers.
- Het EU-initiatief heeft als doel de huidige tekortkomingen op het gebied van digitale identiteit aan te pakken en te zorgen voor een consistente aanpak binnen de hele EU.
- Hoewel de EUDI Wallet voordelen biedt zoals minder accountbeheer en verbeterde privacy, zijn er zorgen over de toegankelijkheid voor alle groepen mensen en de kosten van de infrastructuur.
- De EUDI Wallet, beschikbaar als smartphone-app, stelt gebruikers in staat om identiteitskaarten, licenties, diploma's en andere inloggegevens veilig op te slaan en te delen.
- De toekomst van de EUDI Wallet omvat mogelijke oplossingen voor huidige uitdagingen en de rol van de wallet in de verdere ontwikkeling van de digitale identiteit binnen de EU.

De Europese Digitale Identity (EUDI) Wallet is bedoeld als een veilige en gestandaardiseerde manier voor EU-burgers om identiteitsgegevens op te slaan en te delen. Dit initiatief beoogt een digitale identiteitsinfrastructuur voor alle EU-burgers te creëren. De EUDI Wallet lijkt noodzakelijk om de tekortkomingen van huidige oplossingen aan te pakken en te zorgen voor een gestandaardiseerde en veilige aanpak van digitale identiteit .

In dit artikel schetsen we eerst de trends vanuit het burgerperspectief. Vervolgens bespreken we bestaande oplossingen, privacyaspecten, evenals de uitdagingen. Tot slot beschrijven een mogelijk toekomstbeeld voor de EUDI Wallet.

De Trends

De trend naar digitalisering is alomtegenwoordig en heeft gevolgen voor alle aspecten van ons leven. Bijna alles wat we tegenwoordig doen, vereist een vorm van digitale interactie. Het hebben van een betrouwbare en breed geaccepteerde digitale identiteit om deze digitale interacties uit te voeren is onmisbaar geworden.

Een digitale identiteit wordt verkregen door een account aan te maken dat een bedrijf of instantie aanbiedt. Overheidsinstanties in Nederland bieden daarvoor Digid aan, de banken IDIN en veel andere bedrijven bieden aan om een account per bedrijf aan te maken. Bedrijven en gebruikers hebben verschillende belangen: bedrijven willen hun aanbod verbeteren en markttrends begrijpen, terwijl gebruikers prioriteit geven aan de bescherming en privacy van hun gegevens. Er is sprake van een onbalans. Bedrijven kunnen het creëren van een account afdwingen en vragen bij het aanmaken van het account veel gegevens op. Gebruikers kunnen zonder dat account geen transacties doen en hebben weinig mogelijkheden om verplicht gestelde velden niet in te vullen.

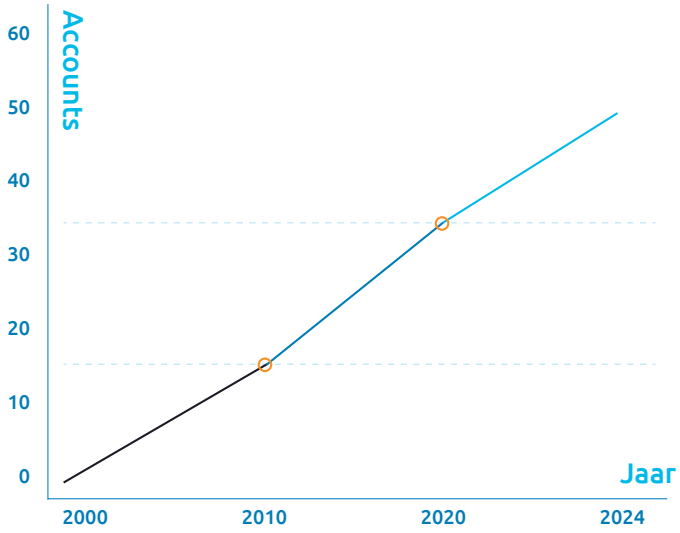
Door deze ontwikkeling groeit het aantal accounts van de gemiddelde Europese burger exponentieel (afbeelding 1). Het onthouden van de wachtwoorden van alle accounts en het regelmatig wijzigen ervan wordt voor de burger een steeds grotere last en dreigt onbeheersbaar te worden. Het bijhouden van welke gegevens aan elk account zijn verstrekt vereist een zorgvuldige administratie, wat veel tijd en moeite kost. En welke privacy en algemene voorwaarden zijn bij het aanmaken van het account geaccepteerd?

Met een digitale identiteit kunnen allerlei zaken worden gedaan waaronder financiële transacties. Het stelen van een digitale identiteit kan daardoor zeer lucratief zijn. Deze identiteitsdiefstal is enorm toegenomen. In 2020 meldde Eurostat dat 4,4% van de Europese burgers te maken had met identiteitsdiefstal. De Europese commissie schatte een financieel verlies van totaal 8,8 miljard euro. In de Verenigde Staten werden in 2022 ruim 1 miljoen gestolen identiteiten gemeld.[1]

We kunnen drie zaken constateren. Ten eerste dat een digitale identiteit noodzakelijk is in de moderne maatschappij. Ten tweede dat het aantal digitale accounts voor de gemiddelde burger onbeheersbaar wordt. En ten derde dat de bedreigingen voor een digitale identiteit toenemen. Tijd om de mogelijke oplossingen te beschouwen!

De trend naar digitalisering is alomtegenwoordig en heeft gevolgen voor alle aspecten van ons leven. Bijna alles wat we tegenwoordig doen, vereist een vorm van digitale interactie.

Afbeelding 1: *Statistisch overzicht van het gemiddelde aantal accounts van de Europese burgers*[2]



Een andere mogelijkheid om rekening mee te houden is het gebruik van een e-wallet. Er bestaan een aantal e-wallets in Europa. Sommige ondersteunen slechts één specifiek doel, zoals inloggen bij de overheid (digid) en betalingen (De digitale portemonnee die veel banken aanbieden, PayPal en Alipay).

Bestaande Oplossingen

Er bestaan momenteel al verschillende oplossingen, maar zijn deze adequaat?

Sociaal inloggen

Het gebruik van social login (door aanbieders zoals Google, Facebook en X) in plaats van het aanmaken van een nieuw account is in Europa populairder geworden. In 2020 gaf ongeveer 80% van de geïnterviewde gebruikers de voorkeur aan het gebruik van social login bij het aanmaken van een nieuw account. Het concept is eenvoudig: u kunt uw bestaande account gebruiken en hoeft geen nieuw account aan te maken.

Een aantal voordelen zijn:

- **Gebruiksgemak;**
  er hoeft geen nieuw account aangemaakt te worden en geen wachtwoorden te worden onthouden.
- **Snelheid;**
  het gaat sneller omdat er geen formulieren ingevuld moeten worden.

Enkel nadelen zijn:

- **Privacy;**
  gebruikers verstrekken hun privégegevens van sociale-mediaplatforms aan websites door in te loggen met een sociale login, en ook aan het sociale platform zelf. Omdat deze systemen gebaseerd zijn op een gecentraliseerde architectuur, is de aanbieder altijd betrokken bij het faciliteren van alle transacties. Hierdoor heeft de sociale inlogprovider inzicht in alle transacties. Indien deze gegevens niet zorgvuldig worden beheerd, kunnen er privacy problemen ontstaan.
- **beveiliging;**
  als de veiligheid van het sociale media-account wordt geschonden, kunnen ook alle accounts die daaraan zijn gekoppeld via sociale login kwetsbaar worden.

[1] Consumer Affairs
[2] https://www.pewresearch.org/internet/2023/10/18/how-americans-protect-their-online-data/ https://www2.deloitte.com/dk/da/pages/technology-media-and-telecommunications/topics/digital-consumer-trends.html https://www.statista.com/statistics/1428413/online-subscriptions-europe/ https://support.nordvpn.com/hc/en-us/articles/19476515228305-How-many-devices-can-I-use-with-NordVPN https://support.surfshark.com/hc/en-us/articles/360003069434-How-many-devices-can-I-use-with-Surfshark-simultaneously

Het gebruik van sociale accounts kan weliswaar een verbetering zijn in het beheer van veel verschillende accounts, maar heeft ook serieuze nadelen. De bestaande oplossing lost het huidige probleem niet op.

Bestaande e-wallets

Een andere mogelijkheid om rekening mee te houden is het gebruik van een e-wallet. Er bestaan een aantal e-wallets in Europa. Sommige ondersteunen slechts één specifiek doel, zoals inloggen bij de overheid (digid) en betalingen (De digitale portemonnee die veel banken aanbieden, PayPal en Alipay).

Meer algemeen toepasbare e-wallets bestaan ook al enige tijd en worden bij bedrijven steeds populairder. Steeds meer websites ondersteunen bijvoorbeeld Yivi en de e-wallet van KPN.

De bestaande e-wallet aanbieders zijn goed in het beschermen van privacy, leveren gebruiksgemak en zorgen dat voor transacties zo min mogelijk gegevens worden uitgewisseld met de aangesloten bedrijven. Door de decentrale infrastructuur wordt voorkomen dat één enkele partij toegang heeft tot alle transacties. Dit systeem biedt gebruikers ook inzicht in het gebruik van hun gegevens door middel van historische overzichten.

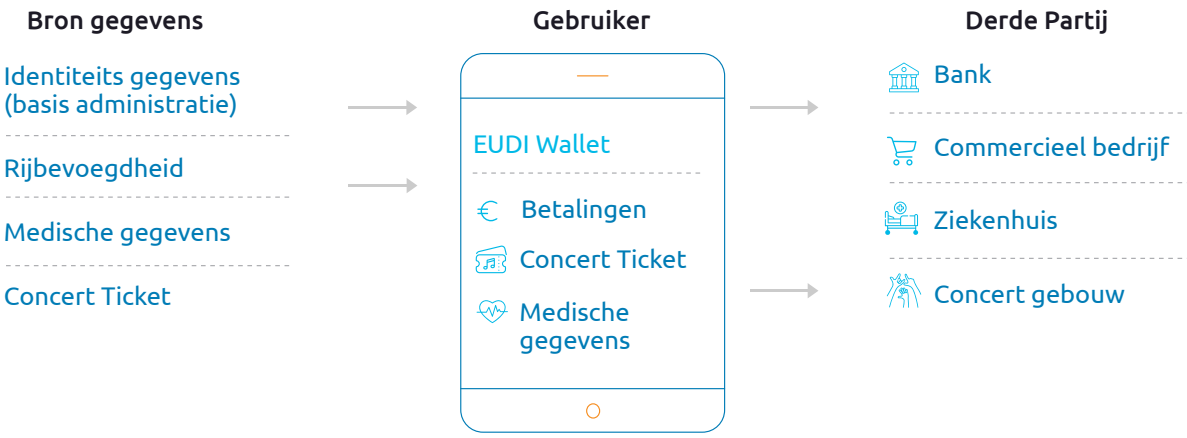
Het proces om een digitale identiteit aan te maken moet wel aan hoge eisen voldoen. Hoewel aanbieders streven naar eenvoud, kan het enige tijd duren om dit proces te doorlopen. Steeds meer bedrijven accepteren deze e-wallets, en het aantal gebruikers neemt gestaag toe.

Het gebruik van de huidige e-wallets is een verbetering ten opzichte van het hebben van afzonderlijke accounts. Behalve het onboardingsproces is het gebruik van de e-wallet niet ingewikkeld en zijn de geboden functionaliteit en beveiligingscontroles beter dan de gemiddelde gebruiker kan uitvoeren.

De EUDI Wallet

De EUDI Wallet is een initiatief van de Europese Unie om een digitale identiteitsinfrastructuur voor alle EU-burgers te creëren. Het doel is om een veilige en gestandaardiseerde manier te bieden om identiteitsgegevens op te slaan en te delen, zie afbeelding 2.

Afbeelding 2:
Statistisch overzicht van het gemiddelde aantal accounts van de Europese burgers



De gebruiker van de wallet kan deze vullen met informatie afkomstig van betrouwbare bronnen, zoals overheidsinstanties. Wanneer je als gebruiker een transactie wilt uitvoeren met een derde partij (in de literatuur vaak aangeduid als de “Relying Party”), kun je een deel van deze gegevens delen met die partij. Dit kan ook een overheidsinstantie zijn.

De EUDI Wallet is niet zomaar een op zichzelf staande app, maar maakt deel uit van een compleet ecosysteem dat zorgt voor een veilige werking. Dit is weergegeven in het schema van afbeelding3.

De Europese Commissie en het Europees Parlement streven naar de ontwikkeling van een Europese gemeenschappelijke digitale markt, met een sterke focus op het beschermen van de privacy van gebruikers.

Hoewel de constructie wellicht complex lijkt, is deze bedoeld om:

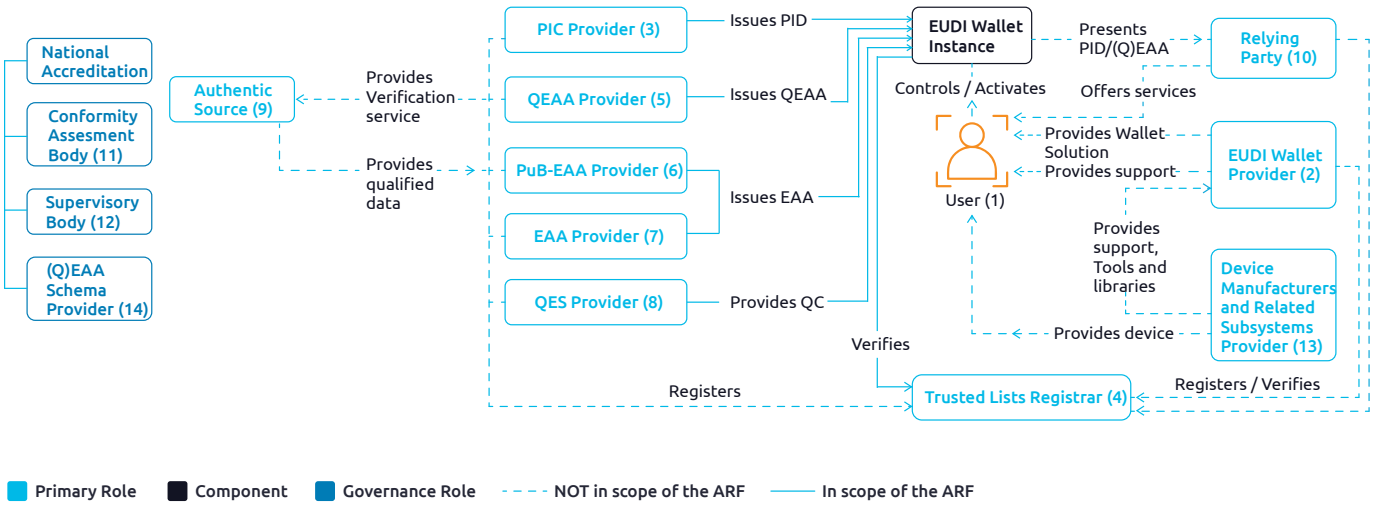
- De machtsverhouding tussen de gebruiker en een commerciële partij in balans te houden
- De privacy van gebruikers te waarborgen
- Instanties die erop toezien en bewaken dat alle partijen zich aan de regels houden.

De EUDI Wallet bestaat in de vorm van een app die op een smartphone kan worden gedownload. Vanaf dat moment kunnen gebruikers veilig verschillende soorten informatie opslaan, zoals identiteitskaarten, rijbewijzen, diploma’s, relevante medische informatie en andere inloggegevens.

Wanneer andere partijen de identiteit en attributen van de gebruiker willen verifiëren, kan de gebruiker de attributen eenvoudig vanuit de EUDI Wallet delen.

Wanneer andere partijen de identiteit en attributen van de gebruiker willen verifiëren, kan de gebruiker de attributen eenvoudig vanuit de EUDI Wallet delen.

Afbeelding 3: *Het EUDI Wallet Ecosysteem*[3]



[3] De complete uitleg kan hier gevonden worden: GitHub: https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/1.4.0/arf/

In de eiDas 2.0 verordening is opgenomen dat zo min mogelijk gegevens mogen worden opgevraagd. Het is afhankelijk van het type transactie welke data daarvoor gebruikt mag worden. Er is een richtlijn opgesteld om partijen te helpen deze minimale dataset te definiëren. In ieder geval moet er sprake zijn van doelbinding, moet de verwerking proportioneel zijn ten opzichte van het beoogde doel, en moet de opslagtijd zo kort mogelijk worden gehouden.

De EUDI Wallet is in alle EU-lidstaten te gebruiken voor publieke en private diensten. De ambitie is om dit verder uit te breiden naar landen buiten de EU.

De EUDI Wallet biedt ontegenzeggelijk voordelen, maar er is ook kritiek te leveren. Een belangrijk punt van kritiek is dat de basis van de EUDI Wallet een mobiele telefoon zal zijn. Deze telefoon moet modern genoeg zijn om aan de beveiligingseisen van de EUDI Wallet te voldoen. Als alleen dure mobiele telefoons aan deze eisen kunnen voldoen, zou een deel van de Europese bevolking mogelijk worden uitgesloten, omdat zij zich zo'n telefoon niet kunnen veroorloven.

Het uitsluiten van groepen doet zich ook voor bij mensen met een beperking en ouderen die de digitale vaardigheden missen om met de EUDI Wallet om te gaan. Het is belangrijk om deze kwetsbare groepen te identificeren en identificeren welke uitdagingen er zullen zijn binnen deze groepen. Er moeten nog oplossingen worden gevonden. Een mogelijke aanpak is het servicemodel, waarbij diensten op een manier worden aangeboden die vergelijkbaar is met een menukaart. In dit model kunnen gebruikers kiezen uit verschillende diensten die aansluiten bij hun behoeften en mogelijkheden. Een voorbeeld hiervan is een gebruiksvriendelijke interface voor ouderen, of speciale ondersteuning voor mensen met een visuele beperking. Dit model kan ook fysieke ondersteuning omvatten, zoals hulp in gemeenschapscentra of bibliotheken waar medewerkers kunnen assisteren bij het gebruik van de EUDI Wallet.

Quote van Margarethe Vestager:

De Europese digitale identiteit stelt ons in staat om in elke lidstaat te doen wat we thuis doen, zonder extra kosten en met minder obstakels. Of het nu gaat om het huren van een appartement of het openen van een bankrekening buiten ons eigen land, dit kan op een veilige en transparante manier. We kunnen zelf bepalen hoeveel persoonlijke informatie we willen delen, met wie en voor welk doel. Dit is een unieke kans om ons allemaal beter te laten ervaren wat het betekent om in Europa te leven en Europeaan te zijn.

Het toevoegen van de EUDI Wallet zal dat belang alleen maar vergroten. Het verlies of diefstal van een smartphone kan voor gebruikers een nachtmerrie worden.

Verder, moet het gebruik van de EUDI Wallet volgens de eiDas regels gratis zijn. De benodigde infrastructuur, inclusief de uitgevende partijen, zal kostbaar zijn en moet zodanig gefinancierd worden dat alle partijen een positieve business case hebben.

Kortom, het beschikbaar hebben van alle data die zowel door overheidsinstellingen als door commerciële partijen geaccepteerd wordt, zal voor de gebruiker ongetwijfeld een groot voordeel opleveren - geen vervelende accounts meer om te onthouden of onveilige opslag van gebruikersgegevens. De EUDI Wallet heeft de potentie om de hoeksteen te worden voor een bloeiende digitale samenleving.

Toekomstbeeld

De bezorgdheid dat de overheid mogelijk inzicht zou kunnen krijgen in alle transacties van gebruikers via de EUDI Wallet, wat zou kunnen leiden tot een “big-brother” effect, vormt een belangrijk obstakel voor de succesvolle werking van de EUDI Wallet. Actiegroepen hebben daarom hun verzet tegen de EUDI Wallet geuit. Om dit tegen te gaan, moeten transparantie en strikte naleving van privacyregels centraal staan in de ontwikkeling en implementatie van de EUDI Wallet.

De smartphone wordt voor de gebruiker de spil om deel te nemen aan de digitale samenleving. Momenteel is de smartphone onze belangrijkste verbinding met de wereld: we gebruiken het om nieuws te consumeren, ons sociale leven bij te houden en als middel voor commerciële bedrijven en overheidsinstellingen om tweefactorauthenticatie te gebruiken voor de beveiliging van het gebruikersaccount. Daarnaast fungeert het ook als onze betaalportemonnee en, zoals bleek tijdens de Covid-pandemie, in sommige gevallen als ons identificatieapparaat.

Het toevoegen van de EUDI Wallet zal dat belang alleen maar vergroten. Het verlies of diefstal van een smartphone kan voor gebruikers een nachtmerrie worden. Om dit probleem te verminderen, kunnen bedrijven investeren in wearables die specifieke functies van de smartphone dupliceren. Het ontwikkelen van wearables die de functies van de EUDI Wallet kunnen beheren en aantrekkelijk zijn voor gebruikers, kan een oplossing bieden. Deze wearables kunnen vervolgens worden gekoppeld aan een 'goedkopere' smartphone, waardoor de afhankelijkheid van één apparaat wordt verminderd.

Andere bedrijven zullen investeren in 'back-up en herstel'-diensten om de identiteit van de gebruiker te herstellen wanneer deze kwijtraakt of wordt gestolen. Dit kan inclusief helpdesk die klachten behandelen wanneer bedrijven of instellingen zich niet aan de regels houden. Deze diensten moeten gebruiksvriendelijk en toegankelijk zijn, zodat alle gebruikers, ongeacht hun technische vaardigheden, snel en efficiënt geholpen kunnen worden.

Tot slot: Kunnen we zonder de EUDI Wallet?

In mijn visie is het antwoord nee. Deelname aan de digitale samenleving zonder een goed beschermde digitale identiteit zal onbeheersbaar of zelfs gevaarlijk zijn. De EUDI Wallet is een goed instrument voor het opbouwen van een gezonde Europese digitale markt, we kunnen niet zonder. Door in te spelen op deze uitdagingen en oplossingen te bieden die de zorgen van burgers en bedrijven adresseren, kan de EUDI Wallet een belangrijk instrument worden in het verbeteren van het beheer en de beveiliging van digitale identiteiten in Europa.

Over de auteurs:

Peter Hoogendoorn

IAM Managing consultant

Peter heeft 12 jaar ervaring als IAM- en beveiligingsconsultant bij diverse bedrijven. Hij heeft speciale interesse in innovatieve oplossingen die de privacy van gebruikers garanderen. Ook is hij betrokken geweest bij een 'privacy by fundament' oplossing waar ook Octrooi op is verleend.

www.linkedin.com/in/petermhoogendoorn

Peter.hoogendoorn@capgemini.com

Roy van der Koogh

Identity & Access Specialist

Roy is een IAM-professional en SailPoint-expert. Begonnen als Business Analist, nu gespecialiseerd in het implementeren van IAM-oplossingen en adviseren van organisaties. Hij heeft een sterke focus op het verbeteren van beveiliging en efficiëntie.

www.linkedin.com/in/royvanderkoogh/

roy.vander.koogh@capgemini.com

07

SecDevOps-processen implementeren terwijl teams het niet willen

Hoe kan agile-ontwikkeling bijdragen aan consistentie en ervoor zorgen dat teams aan dezelfde beveiligingseisen voldoen?

Highlights

- Het laten volgen van één set richtlijnen door verschillende ontwikkelingsteams is een uitdaging.
- Agile-ontwikkeling dwingt organisaties om een keuze te maken tussen functionaliteit en beveiliging.
- Kerst 2021 en log4j hebben ons lessen geleerd over het belang van SecDevOps-beleid.
- Wil je dat ontwikkelaars het juiste doen? Maak het dan betaalbaar en eenvoudig.
- De beste manier om te laten zien dat je vooruitgang boekt, is door te meten.

Grote organisaties ondervinden steeds meer druk om al hun ontwikkelingsteams de basis vereisten voor security te laten volgen. Gelukkig hebben we op dit vlak een aantal lessen geleerd waarmee iedereen zijn voordeel kan doen – mits je een goed plan uitstippelt.

Naleving en bewustzijn van cybersecurity zijn drijvende krachten achter de beveiliging van organisaties. Het besef is gegroeid dat aandacht hebben voor beveiliging tijdens de softwareontwikkeling de cybersecurity-risico's kan verminderen. Het introduceren van nieuw beveiligingswerk in een project is moeilijk, maar het introduceren van nieuwe vereisten aan meerdere ontwikkelingsteams binnen een groot bedrijf maakt het nog moeilijker.

Waarom is SecDevOps belangrijk?

Hoe eerder je beveiliging introduceert, hoe lager de kosten. Daarom wordt beveiliging door SecDevOps toegepast tijdens de volledige ontwikkelingslevenscyclus. Dit betekent dat het product ontworpen moet worden om veilig te zijn. De ontwikkeling omvat veilige codebeoordelingen, codescanning, statische analysetools (SAST) en dynamische analysetools (DAST). Ter voorbereiding op toekomstige kwetsbaarheden wordt er een Software Bill of Materials (SBOM) opgesteld. Operationeel wordt een veilige implementatie uitgevoerd die verkeerde configuratie en de installatie van malware moet voorkomen. Operationele teams moeten erop berekend zijn dat kwetsbaarheden worden gevonden en beveiligingsincidenten dienovereenkomstig monitoren. Een DevOps-proces is cyclisch en SecDevOps is een natuurlijke uitbreiding die naadloos integreert in geautomatiseerde CI/CD-pijplijnen.

Agile vs. SecDevOps

Agile werd zo'n vijftien jaar geleden ineens op grote schaal geadopteerd binnen de softwareontwikkeling. Hoewel het niet altijd op een consistente manier wordt gebruikt, verwachten ontwikkelingsteams inmiddels wel regelmatige releases van werkende software en een nauwere band met eindgebruikers.

Sommige principes van Agile-ontwikkeling kunnen bijdragen bij beveiliging:

- Veranderende vereisten moeten omarmd worden, zoals de implementatie van nieuwe beveiligingsmaatregelen.[1] Projecten worden neergezet vanuit gemotiveerde individuen. Elk teamlid kan invloed hebben op hoe beveiliging benaderd wordt.
- De cyclische aard van Agile maakt het gemakkelijk om SecDevOps-praktijken te integreren.

Maar de Agile-principes kunnen ook tegen ons werken:

- Klanten tevreden stellen is cruciaal. Vaak verwachten klanten dat beveiligingsfuncties standaard aanwezig zijn. Daarmee kan de implicatie gewekt worden dat de systemen hiervoor niet veilig waren en daar niets over gezegd is.
- Bedrijfseigenaren en ontwikkelaars werken samen met een focus op Return on Investment (ROI). Beveiligingsinvesteringen verminderen risico's, wat niet hetzelfde is als ROI en moeilijker te begrijpen. Werkende software is de primaire maatstaf voor vooruitgang, terwijl beveiligingscontroles worden vaak gezien als obstakels voor (nieuwe) features.
- Maar het grootste obstakel is de Agile-waarde die meer waarde hecht aan individuen dan aan processen en tools. SecDevOps zijn fundamenteel nieuwe processen. Veel compliance-frameworks hebben specifieke vereisten voor softwareontwikkeling, zoals ISO 27002 sectie 8 en PCI Secure Software Framework. Het voldoen aan deze vereisten houdt in dat nieuwe SecDevOps-beleidslijnen worden gevolgd.

Kerst 2021: toen we het belang van SecDevOps-beleid leerden[2]

In november werd er een kritieke kwetsbaarheid genaamd Log4jShell gevonden in een veelgebruikte bibliotheek genaamd log4j. Dit logging framework was de afgelopen tien jaar veelvuldig gebruikt in applicaties. Het repareren was een uitdaging omdat het vaak werd ingeladen door verschillende bibliotheken die ook bijgewerkt moesten worden. Die kerstperiode werd besteed aan het identificeren van noodzakelijke updates en het maken van kleine aanpassingen die hopelijk de functionaliteit niet zouden verminderen. Dit leidde tot nieuwe bugs die verholpen moesten worden, vaak in code die al jaren niet was aangeraakt.

Agile methodes bewezen hun nut in deze periode. Teams konden snel reageren op veranderingen door enkele sprints te wijden aan het bijwerken van log4j of het volledig verwijderen ervan. De acceptatie van de veranderingen maakte het makkelijker om ruimte in de planning te maken voor dit werk. Aan de kant

[1] Agile Manifesto - https://agilemanifesto.org/

[2] Log4Shell vulnerability -- https://en.wikipedia.org/wiki/Log4Shell

Zoals de Engelsen het zo mooi formuleren: 'Je kunt een paard naar het water leiden, maar je kunt het niet laten drinken.' Oftewel: uiteindelijk moeten de teams het zelf doen.

van SecDevOps toonden SBOM-tools (en andere) hun waarde. Teams hadden beter inzicht in wat er werd gebruikt en waar. Verandermanagement werd ineens veel belangrijker. In grotere organisaties bleek dat sommige teams beter presteerden dan andere. Het was niet alleen het proces dat waardevol was, maar ook de consistentie. We hoopten dan ook het nieuwe jaar in te gaan met een hernieuwd begrip van de waarde van consistent SecDevOps-beleid.

Waarom het in grotere organisaties moeilijker is

Hoe kunnen we verwachten dat ontwikkelingsteams hun processen standaardiseren en meer stappen toevoegen als Agile juist individualisme prioriteert? De simpele uitleg is dat een CISO of risk officer gewoon kan dicteren dat alle afdelingen aan nieuwe beveiligingseisen voldoen. Hoewel deze aanpak vaak goed werkt in relaties met een rapportagestructuur zoals tussen IT en de CIO of CTO, is de situatie met ontwikkelingsteams zelden zo eenvoudig.

Product owners binnen ontwikkelingsteams worden aangemoedigd om functies te verbeteren. Gebruikers verwachten dat beveiliging al inbegrepen is, dus de waarde van beveiliging wordt niet altijd begrepen. Daardoor geven product owners vaak minder prioriteit aan beveiligingsvereisten, terwijl het risico ligt bij de CISO of risk officer.

Gedeelde platforms als redding: maak het goedkoop en eenvoudig

Zoals de Engelsen het zo mooi formuleren: 'Je kunt een paard naar het water leiden, maar je kunt het niet laten drinken.' Oftewel: uiteindelijk moeten de teams het zelf doen. De makkelijkste manier om hen mee te krijgen, is door in te spelen op de drijfveren van het team – en voor ontwikkelingsteams is dat kostenreductie. Gedeelde platformgroepen kunnen een sleutelrol spelen bij het implementeren van beveiliging. Efficiënte softwareontwikkeling maakt gebruik van code-hergebruik. Door de kosten te verdelen over veel applicaties worden de gemeenschappelijke componenten goedkoper. Als die componenten veel worden gebruikt, neemt ook de kwaliteit toe. Deze kant-en-klare componenten kunnen Python-packages of Kubernetes-container-images zijn. Beveiliging is meestal onderdeel van deze open source componenten. In sommige bedrijven zijn er gemeenschappelijke componenten die specifiek zijn voor dat bedrijf, zoals een authenticatiesysteem dat is geconfigureerd om alleen met de bedrijfsauthenticator te communiceren.

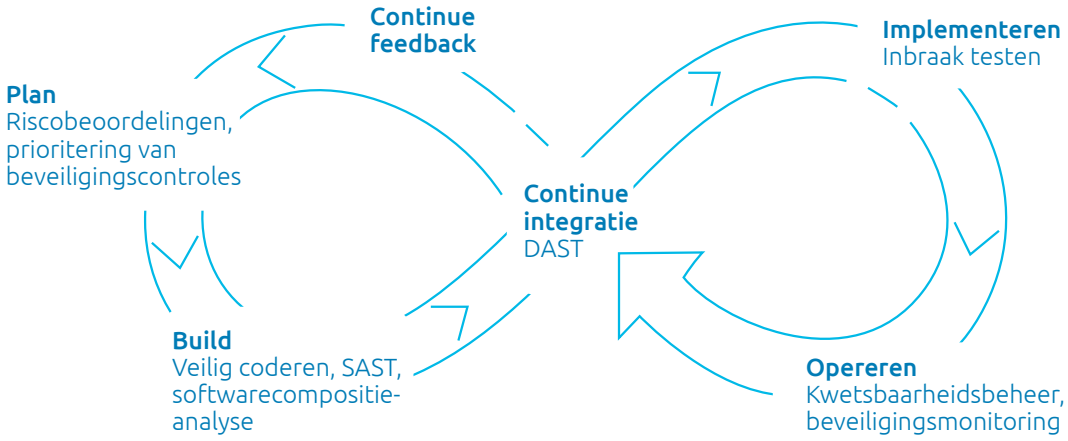
Een efficiënt gerund bedrijf zal een gemeenschappelijke platformgroep hebben die een verzameling van deze componenten samenstelt. Ze controleren ze op beveiligingsfouten, regelen licenties als nodig en voeren tests uit (zoals kwetsbaarheidsscans). Het doel van de gemeenschappelijke platformgroep is om componenten zo overtuigend te maken dat geen enkel applicatieteam ervoor zou kiezen om het zelf te doen. Het kan grote voordelen opleveren als beveiligingscontroles zijn ingebouwd in gemeenschappelijke componenten die door de platformgroep worden ontwikkeld. Als ontwikkelingsteams ze gebruiken, krijgen ze de beveiligingscontroles er namelijk gratis bij. Dit betekent een gerichte investering in het platformteam om veilige componenten te creëren.

Investeren in de beveiligingscapaciteiten in een gemeenschappelijke platformgroep kan een multiplier-effect hebben.

Instrumentatie van CI/CD-pijplijnen

Omdat gedeelde platformteams vaak een geconsolideerde CI/CD-build pijplijn uitvoeren, gebruikt een bedrijf één pijplijn voor verschillende teams. Door de DevOps-vaardigheden in één afdeling te concentreren, is het mogelijk om de kosten te verlagen. Door het integreren van code scanning en kwetsbaarheidsmanagement in deze pijplijnen krijgen ontwikkelingsteams automatisch opsporingscontroles – zelfs als ze daar niet specifiek om hebben gevraagd. Afbeelding 1 toont de verschillende fasen van een DevOps-cyclus en waar beveiligingspraktijken passen.

Afbeelding 1: *SecDevOps-levenscyclus*



Zeker weten dat ontwikkelingsteams begrijpen wat ze moeten doen

De meest effectieve manier om een organisatie te beïnvloeden, is van binnenuit. Een principe van Agile-ontwikkeling is het inzetten van gemotiveerde individuen. Het implementeren van een Security Champions-programma kan daarbij helpen.[3] Ervaring leert dat ongeveer één op de tien engineers van nature om beveiliging geeft, ongeacht de senioriteit of ervaring. Als je de leiding van ontwikkelingsteams vraagt om iemand te nomineren, dan zullen het deze mensen zijn. Zij zijn je bondgenoten. Een Security Champions-programma kan je helpen om deze engineers te vinden. Een Security Champion zelf fungeert als het enige contactpunt voor beveiligingskwesties, vergroot het lokale bewustzijn van beveiliging en levert feedback voor centrale beveiligingsprogramma's. De implementatie van deze rol kan een geweldige groeikans zijn. Een goed programma kan geavanceerde training bieden aan de Champions en feedback verzamelen over de beveiligingsstatus van elk ontwikkelingsteam. Het doel is ervoor te zorgen dat beveiligingsprofessionals zich verbonden voelen door het hele bedrijf.

Maak SecDevOps-programma's meetbaar

Het is belangrijk dat CISO's begrijpen wat hun rendement op beveiligingsinvesteringen is en om compliance en aandachtspunten te meten. KPI's zijn alleen nuttig als ze consistent en relevant zijn. In afbeelding 2 staan enkele voorbeelden van metingen die kunnen worden gebruikt. Het volgende diagram toont een gemeenschappelijke SecDevOps-levenscyclus met de beveiligingsaspecten en markeert de verschillende statistieken die beschikbaar zijn in elke fase.

[3] OWASP Security Champions Guide - https://owasp.org/www-project-security-champions-guidebook/

Rapporten kunnen in verschillende formats worden gepresenteerd. Een dashboard (bijvoorbeeld in PowerBI of ServiceNow) leent zich goed om de huidige status per ontwikkelingsteam weer te geven. Het kan trends in de tijd laten zien die bijvoorbeeld voortuitgang of achteruitgang illustreren. In de ideale situatie ontvangt het senior management ook elk kwartaal een rapport. Deze vorm van transparantie zorgt ervoor dat cyberveiligheid als risico op de agenda van de organisatie wordt gezet.

Ontwikkelingsteams simpelweg instrueren om aan de nieuwe beveiligingseisen te voldoen, is zelden effectief. Het werkt beter als je ervoor zorgt dat beveiligingsaspecten makkelijk te adopteren zijn door ze kosteneffectief te maken. Sommige Agile-principes vormen een uitdaging voor de implementatie van beveiliging, maar ze kunnen deze ook ondersteunen. Het opzetten van een Security Champions-programma kan de beveiligingscultuur in de hele organisatie positief beïnvloeden.

Afbeelding 2: *SecDevOps-statistieken*

Meting	Relevantie
Algemene processen en naveling-validatie	Welke van deze fases zijn geïmplementeerd? Dit meet SSD-adoptie en laat zien of SSD-aspecten worden toegepast.
Threat modelling	Genereert een lijst van bekende risico's binnen een organisatie.
Statische code-analyse	Het aantal acceptabele zwakheden en de ernst ervan kunnen een indicatie geven van het beveiligingsniveau van het ontwikkelingsteam.
Kwetsbaarheidsscan	Toont het risico van producten in gebruik. Trends laten zien of het ontwikkelingsteam de toestroom van CVE's aankan.
Bedrijfsvoering	Succesvolle aanvallen zijn een indicator achteraf voor het niveau van aandacht voor beveiliging.

Over de auteurs:

Alex de Vries

Principal Cybersecurity Consultant

Alex is een security expert met 25 jaar ervaring in software ontwikkeling, gespecialiseerd in embedded systemen en de overstap naar de cloud. Met tien jaar expertise op het gebied van beveiliging richt hij zich op risicobeheer en het waarborgen van robuuste SecDevOps.

www.linkedin.com/in/alexdev-sec/

alex.de.vries@capgemini.com

PUBLICATIES

Naast ons 'Trends in Cybersecurity' rapport publiceren wij nog andere rapporten, onderzoeken en whitepapers die voor u relevant kunnen zijn. Onderstaand treft u een verkort overzicht aan. Het complete overzicht vindt u op: www.capgemini.nl

Trends in Veiligheid 2024-2025 Veiligheid in Society 5.0

Het 14e Trends in Veiligheid rapport is gelanceerd, met als hoofdonderwerp: Veiligheid in Society 5.0. Dit rapport, speciaal samengesteld voor het publieke veiligheidsdomein, biedt waardevolle inzichten vanuit vijf verschillende thema's: Weerbaarheid, Wendbaarheid, Data, Burger centraal en de Toekomst van werk. Lees over de belangrijkste trends om uw organisatie te beschermen, te ontwikkelen en te innoveren in de moderne samenleving.

https://www.capgemini.com/nl-nl/trends-in-veiligheid-2024-2025/

Applications Unleashed The Era of Prompt Innovation

De voortdurend evoluerende technologieën van het afgelopen jaar hebben onze wereld hervormd, waardoor directe bevrediging als vanzelfsprekend is geworden. Maar nu de grenzen van innovatie hun hoogtepunt hebben bereikt, rijst de vraag: Wat staat ons te wachten? Hoe ziet de toekomst van het techlandschap eruit? En hoe zal het onze ondernemingen beïnvloeden? De stabiliteit van onze banen? Hoe zal dit weerspiegelen in onze leefomgeving, en een stempel drukken op ons alledaagse bestaan? Deze vragen worden behandeld in Applications Unleashed 2024, waar concrete voorbeelden uit het dagelijkse leven en praktisch toepasbare inzichten een geëffend pad banen naar de baanbrekende ideeën van de toekomst.

https://www.capgemini.com/nl-nl/applications-unleashed-2024/

Turbocharging software with GenAI Ontdek hoe generatieve AI de toekomst van Software Engeneering bepaalt

In dit rapport van Capgemini Research Institute 'Turbocharging software with GenAI', wordt onderzocht hoe organisaties het volledige potentieel van generatieve AI voor software-engineering kunnen benutten op een manier die beveiligingsrisico's beperkt, prioriteit geeft aan use cases en mensen centraal stelt in deze transformatie.

https://www.capgemini.com/nl-nl/expertise/research/ontdek-hoe-generatieve-ai-de-toekomst-van-software-engineering-bepaalt/

COLOFON

Deze editie van Trends in Cybersecurity is tot stand gekomen met medewerking van:

Natasja Pieterman

Folkert Visser

Joris Commissaris

Ruurd Jorritsma

Thomas de Klerk

Ernes Mahmutovic

Devana Thonhauser

Advies, ontwerp en productie:

Marketing & Communicatie, Capgemini Nederland B.V.

Johanna Achterberg

Ashim Karmakar

Arindam Dey

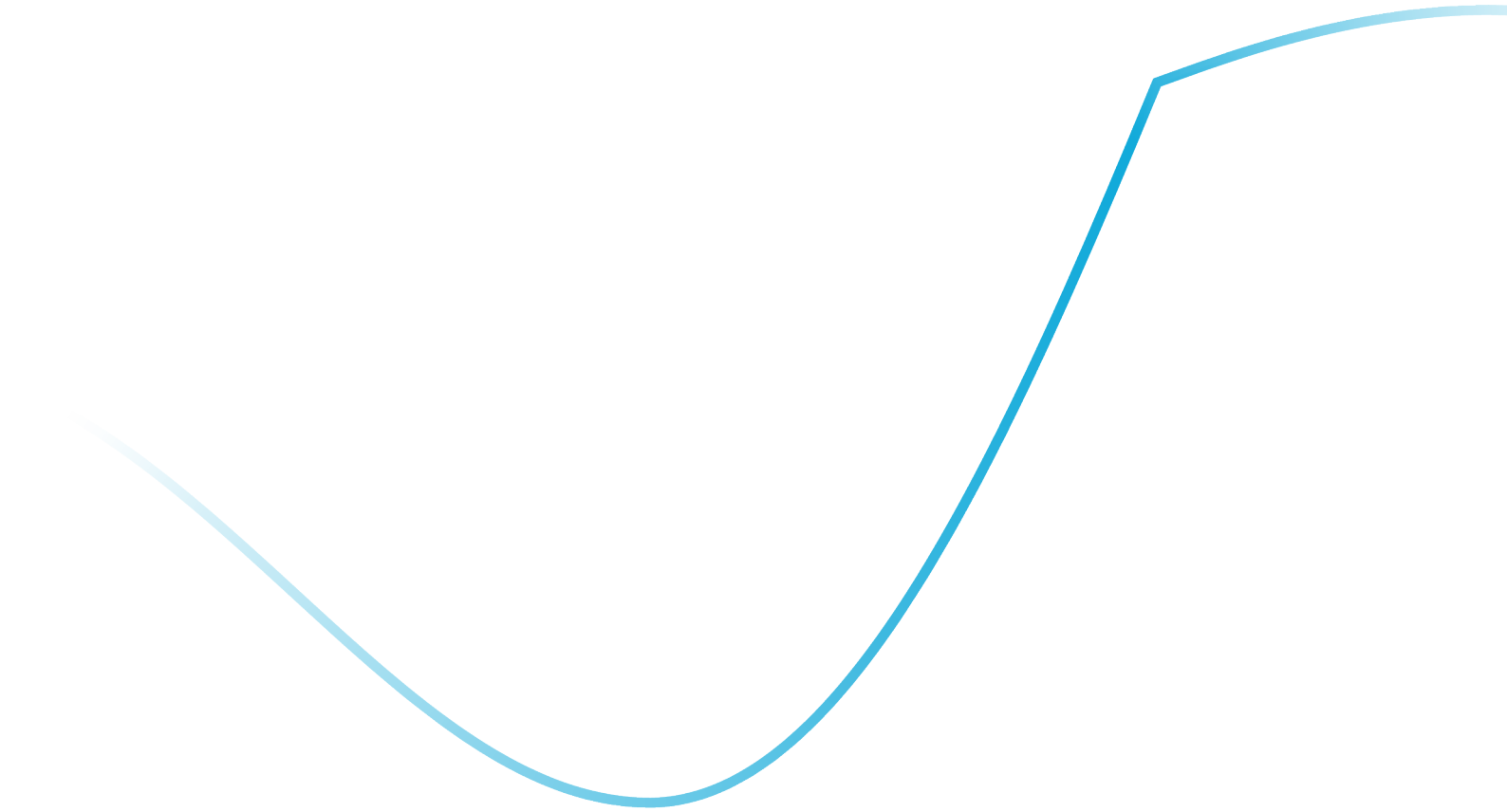
Runa Roychowdhury

Capgemini Nederland B.V.

Postbus 2575 – 3500 GN Utrecht

+31 30 689 00 00

www.capgemini.nl



Over Capgemini

Capgemini is een wereldwijde, maatschappelijk verantwoorde en multiculturele marktleider met 360,000 mensen in bijna 50 landen. Als strategisch partner ondersteunt Capgemini organisaties bij hun transformatie door gebruik te maken van de kracht van technologie. Hierbij laat de Group zich leiden door zijn bestaansreden: menselijke energie vrijmaken door middel van technologie voor een inclusieve en duurzame toekomst. Met meer dan 50 jaar ervaring en expertise in uiteenlopende sectoren, vertrouwen klanten de aanpak van hun zakelijke behoeften toe aan Capgemini: van strategie en ontwerp tot operationeel beheer. Dit gebeurt door gebruik te maken van innovaties in cloud, data, kunstmatige intelligentie, connectiviteit, software, digital engineering en platforms. De Group behaalde in 2022 een omzet van € 22 miljard.

GET THE FUTURE YOU WANT | www.capgemini.nl

2D-030.24

Capgemini Nederland B.V.
Postbus 2575 - 3500 GN Utrecht
Tel. + 31 30 203 05 00
www.capgemini.nl